(9)

Japanese Patent Laid-open No. 2000-293936 A
Publication date : Oct. 20, 2000
Applicant : Hitachi Ltd.
Title : DIGITAL SIGNAL RECORDING APPARATUS, REPRODUCING APPARATUS, AND RECORDING MEDIUM

[0012] Embodiments of the present invention will be explained below with reference to the accompanying drawings.

[0013] Fig. 1 is a configuration diagram including a digital broadcast receiver and a digital signal recording and reproducing apparatus. 200 is a digital signal recording and reproducing apparatus, 201 is a digital broadcast receiving apparatus, 202 is an antenna, 207 is a receiver, 203 is a tuner, 204 is a selection circuit, 205 is a decryption circuit, 206 is an interface circuit, and 208 is a control circuit for controlling operations of the digital broadcast receiver 201. Although the digital broadcast receiver 201 and the digital recording and reproducing apparatus 200 are shown as being separate, they can be integrated.

[0014] Fig. 2 is a configuration diagram of the digital signal recording and reproducing apparatus 200 in Fig. 1. Although the apparatus in Fig. 2 is used for both recording and reproducing, it is the same even if the recording and reproducing are configured to be independent. 100 is a rotating head, 101 is a capstan, 102a is a recording signal processing circuit for performing generation or the like of a recording signal at the time of recording, 102b is a reproduction signal processing circuit for demodulation or the like of the reproduction signal at the time of reproduction, 104 is a control circuit, for example, like a microprocessor, which controls of the recording and

reproduction modes or the like, 105 is a timing generation circuit for generating a timing signal that becomes the reference for rotation of the rotating head 100 or the like, 106 is a servo circuit for controlling the rotating head and the feed speed of the tape, 107 is an input and output circuit for inputting the recording signal or outputting the reproduction signal, 109 is a timing control signal for controlling the timing at the time of recording, 110 is an oscillating circuit for generating a reference clock, 111 is a tape, 112 is a recording and reproduction circuit of the analog video signals, 115 is a data encryption circuit at the time of digital signal recording, 116 is a data decryption circuit at the time of digital signal reproduction, 117 is a device key generator for generating a device key that becomes the basis of the data key that is supplied to the data encryption circuit 115 or a data decryption circuit 116 when digital information is encrypted or decrypted, 118 is a block key generator for generating the block key that is another basis of the data key when digital information is encrypted or decrypted, and 119 is an input and output control circuit for performing time stamp processing of packet data at the time of recording and for performing output control of the packet data at the time of reproduction.

[0015] The digital video compressed signal is sent as packet data by time-division multiplexing the signals of multiple channels. In Fig. 1, the digital broadcasting signal received by the antenna 202 is demodulated by the tuner 203, and then the necessary digital compressed image signal is selected by the selection circuit 204. The selected digital compressed image signal is decrypted into a normal video signal by the decryption circuit 205 and inputted into the receiver 207. When processing such as

scrambling or the like is performed on the reception signal, decryption processing is performed in the selection circuit 204 after a process such as scrambling or the like is cancelled. When recording of the received digital broadcast signal is performed, the digital compressed video signal to be recorded and information relating thereto are selected in the selection circuit 204, inputted into the digital signal recording and reproducing apparatus 200 by the input and output terminal 108 of the digital signal recording and reproduction apparatus via the interface circuit 206 and recorded. When reproduction of the recorded digital broadcast signal is performed, the digital compressed image signal or the like reproduced by the digital signal recording and reproduction apparatus 200 is outputted to the interface circuit 206 by the input and output terminal 108. Processes similar to those normally performed at the time of reception are performed on the digital compressed video signal or the like inputted into the interface circuit 106 by the selection circuit and the decryption circuit, and the digital compressed video signal is then outputted to the receiver 207.

[0016] In Fig. 2, which depicts the configuration of the digital signal recording and reproducing apparatus 200 in Fig. 1, a part of the packet data inputted by the input and output terminal 108 is inputted into the control circuit 104 via the input and output circuit 107 at the time of recording. In the control circuit 104, the type of packet data and the like is detected by information attached to the packet data or information that has been sent separately to the packet data, the recording mode is determined by the detection result, and the operation modes of the recording signal processing circuit 102a and the servo circuit 106 are set. The input and output circuit

107 then outputs to the data encryption circuit 115 the packet data to be recorded. In the data encryption circuit 115, by generation of the data key in the control circuit 104 based on the key to be generated by the device key generator 117 and the block key generator 118, the packet data is encrypted and the encrypted packet data is outputted to the input and output control circuit 119. In the input and output control circuit 119, based on the timing information from the timing generation circuit 105, the time stamp is given to the inputted packet data and the inputted packet data given the time stamp is outputted to the recording signal processing circuit 102a. In the recording signal processing circuit 102a, according to the recording mode determined by the control circuit 104, the generation of recording data such as the error correction decryption, the ID information, the sub-code, the block key information used in encryption, and the like is performed and the recording signal is generated, which is recorded onto the tape 111 by the rotating head 100.

[0017] At the time of reproduction, a reproduction operation is firstly performed in an optional reproducing mode and the ID information is detected by the reproduction signal processing circuit 102b. It is determined by the control circuit 104 as to what mode recording has been performed in and reproduction is performed by resetting the operation modes of the reproduction signal processing circuit 102b and the servo circuit 106. In the reproduction signal processing circuit 102b, the detection of the synchronization signal, the correction of error detection, and the acquisition of block key information or the like are performed from the reproduction signal reproduced by the rotating head 100 and the packet data is outputted to the input and output control circuit 119 after

being reproduced. In the input and output control circuit 119, the packet data free of the time stamp is outputted to the data decryption circuit 116 as the reference of the timing generated by the timing generation circuit 105. In the data decryption circuit 116, based on the key generated by the device key generator 117 and the block key obtained by the reproduction, the packet data free of the time stamp is decrypted by the data key generated in the control circuit 104 and outputted to the input and output circuit 107.

[0018] At the time of recording, the operation timing of the recording and reproducing apparatus is controlled by the timing control circuit 109 as the reference of the rate of recording data inputted by the input and output terminal 108. At the time of reproduction, an oscillated clock is operated by the oscillating circuit 110 as the reference of the operation.

[0019] Fig. 3 is a configuration diagram of the packet of the digital video compressed signal. One packet is constituted of a fixed length, for example, 188 bytes, and includes a 4-byte packet header 306 and 184-byte packet information 307. The digital compressed video signal is positioned in the region of the packet information 307. The packet header 307 is constituted of information such as the type of packet information.

[0020] Fig. 4 is a configuration diagram of the packet header 306 in Fig. 3. 501 is a synchronization byte indicating the head of the packet, 502 is an error display indicating presence of an error, 503 is a unit start display indicating a start of a unit, 504 is packet priority indicating the importance of the packet, 505 is a packet ID indicating the type of a packet, 506 is scrambling control indicating the presence of scrambling,

507 is adaptation field control indicating presence of additional information and presence of packet information, and 508 is a checking counter for counting up in packet units.

[0021] Fig. 5 is a configuration diagram of transmitted signals of the digital broadcast and the signals selected from the transmitted signals. 71 is a packet in Fig. 3. Normally, the sound signal, information relating to a program, and the like are attached to the video signal mentioned above. Programs of multiple channels are transmitted by time-division multiplexing.

[0022] Fig. 5(a) is an example of a multiplexed three channel program. V1, V2, and V3 are video signals for the respective channels and A1, A2, A3 are packets of the sound signals for the respective channels. A single channel can be constituted of multiple videos and sounds. P0, P1, P2, and P3 are information relating to the programs. A different packet ID 505 is allocated to each packet. Thus, identification of packet's contents can be done.

[0023] P0 is information relating to the whole of the transmitted signal in Fig. 5(a). Packets such as the program association table for identifying as to what packet ID is allocated to each program and the program guide information are transmitted by time-division multiplexing. P1, P2, and P3 are information relating to the respective programs. Packets such as a program map table for identifying which packet IDs have been allocated to the video packet, the sound packet, and the like of the channels and scrambling information are transmitted by time-division multiplexing. Normally, a determined value, for example, 0, is allocated to the packet ID of the program association table.

[0024] At the time of reception, it is firstly

recognized by the program association table as to what packet ID has been allocated in the program map table for the program desired to be received. It is then recognized by the program map table of the program desired to be received as to what packet IDs have been allocated to the video packet, the sound packet, and the like. Decryption of the digital compressed data is performed by extracting the video packet and the sound packet. The program clock reference is extracted at the same time. Thus, the operation of the decryption circuit is controlled so that the decryption timing of the decryption circuit of the digital compressed data is in synchronization with the time of encryption.

[0025] CR is program clock reference information in order to be in synchronization with the time of decrypting the digital compressed data.

[0026] Of course, the number of channels to be multiplexed can be other than three channels, for example, four channels. Other pieces of information can also be multiplexed.

[0027] Fig. 5(b) is only the information selected from the first channel from Fig. 5(a) and program information relating thereto. When the first channel is recorded, this information is outputted to the recording and reproducing apparatus 200 from the digital broadcast receiver 201. Information other than this can be recorded. In order to facilitate processing at the time of reproduction, a part of the packet information can be changed. For example, if the packet information is changed to only information of the program for recording program association table information, channel selection is unnecessary at the time of reproduction.

[0028] Fig. 6 is a configuration diagram of the data

encryption circuit 115 in Fig. 2. 1151 is a packet data input terminal, 1157 is a packet data output terminal, 1153a and 1153b are data key input terminals, 1153c is a data key selection signal input terminal, 1153d is a processing mode selection signal input terminal, 1152 and 1156 are block processing circuits, 1154 is a key schedule circuit, 1155 is an encryption device, 1158a and 1158b are data key registers, and 1159 is a data key selector. The data encryption circuit 115 outputs by encrypting inputted packet data units by a data key determined in advance. The stability of the packet data being recorded onto a tape can be increased by the data key being changed at a certain time interval.

[0029] In the encryption device 1155, for example, even if an error such as a bit error occurs during transmission, the error has no influence on the following data. In other words, so there is no error propagation, a block encryption that can realize encryption processing by a simple circuit configuration for a block constituted of multiple bits is used by the encryption device 1155.

[0030] The packet data inputted from the input terminal 115 is firstly segmented into block P including multiple bits in the block processing circuit 1152. For example, one block is 64 bits. Each block is sequentially encrypted in the encryption device 1155. The block C is thus outputted and in the block processing circuit 1156, the block is returned to the form of packet data and outputted to the output terminal 1157. The data key, which is the key for encryption, is inputted from the data key input terminals 1153a and 1153b by the control circuit 104 and stored in the data key registers 1158a and 1158b. For example, the present data key is recorded in the data key register 1158a and the data key to be switched to next is

recorded in the data key register 1158b.

[0031] The signal for indicating which of either the data key register 1158a or 1158b is to be selected is inputted by the control circuit 104 and the selected data key is outputted by the data key selector 1159 from the data key selection signal input terminal 1153c. For example, the data key of the key register 1158a is selected. The selected data key is changed to sub keys KA and KB in the scheduling circuit 1154 and supplied to the encryption device 1155. For example, the length of the data key is 56 bits and the length of each sub keys is 32 bits. The top 32 bits of the data key are allocated to KA and the additional value of the top 32 bits and the bottom 32 bits of the data key are allocated to KB.

[0032] When the data key is changed, a signal is inputted from the data key selection signal input terminal 1153c by the control circuit 104 so that the data key register 1158b will output. The data key selector does not switch the selected output until the encryption of the blocks for one packet data has completely finished and is controlled so as to switch between packet data.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－293936
（P2000－293936A）
(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
	３０１		３０１Ｚ	５Ｄ０４４
20/12	１０２	20/12	１０２	
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	
5/92		5/92	Ｈ	

審査請求　未請求　請求項の数28　ＯＬ　（全 28 頁）

(21)出願番号　特願平11－100976

(22)出願日　平成11年４月８日(1999.4.8)

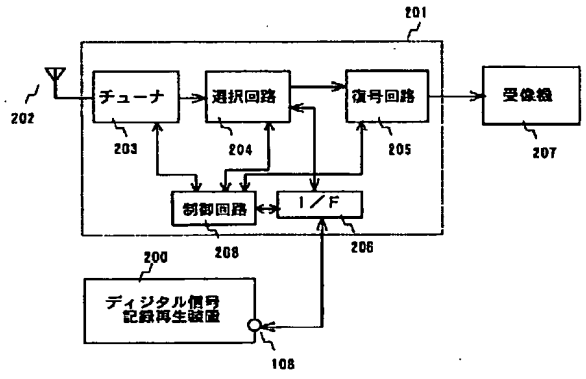
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　佐々本　学
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ディジタル信号記録装置、再生装置、および記録媒体

(57)【要約】
【課題】記録媒体上のディジタル信号の著作権を保護できる記録装置、再生装置、および記録媒体を提供することにある。
【解決手段】ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力することにより達成できる。

図１



1

【特許請求の範囲】

【請求項１】ディジタル信号を記録媒体上に記録するディジタル信号記録装置において、
少なくとも一つの鍵情報を発生する鍵情報発生手段と、前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするディジタル信号記録装置。

【請求項２】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項１記載のディジタル信号記録装置。

【請求項３】前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を備え、前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記記録媒体上の所定の領域に記録する機能を備えたことを特徴とする請求項１記載のディジタル信号記録装置。

【請求項４】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項３記載のディジタル信号記録装置。

【請求項５】前記暗号変換手段は、さらに、前記ディジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を備え、
前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求項１記載のディジタル信号記録装置。

【請求項６】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項５記載のディジタル信号記録装置。

【請求項７】所定長のディジタル信号を入力して、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第１の誤り訂正符号を付加し、さらにｎ（ｎは１以上の整数）セクタ単位で第２の誤り訂正符号を付加し、前記第２の誤り訂正符号にも第１の誤り訂正符号を付加して記録媒体上に記録するディジタル信号記録装置において、

2

少なくとも一つの鍵情報を発生する鍵情報発生手段と、前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするディジタル信号記録装置。

【請求項８】前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を有し、前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、前記所定の演算を行って更新された鍵を発生し、
前記暗号変換手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で、前記更新された鍵に切り換える機能を備えたことを特徴とする請求項７記載のディジタル信号記録装置。

【請求項９】前記暗号変換手段は、前記ディジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を有し、
前記記録手段は、前記ディジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、
前記第２の誤り訂正符号を付加したセクタの単位の区切り目で、前記ディジタル信号を暗号化するか否かを切り換える機能を備えたことを特徴とする請求項７記載のディジタル信号記録装置。

【請求項１０】記録媒体上に記録されているディジタル信号を再生するディジタル信号再生装置において、
前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするディジタル信号再生装置。

【請求項１１】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項１０記載のディジタル信号再生装置。

【請求項１２】少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、
前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力されて所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。

【請求項１３】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情

報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。

【請求項１４】前記ディジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記ディジタル信号の各パケットに付加して記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求項１３記載のディジタル信号再生装置。

【請求項１５】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備え、

前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。

【請求項１６】前記ディジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記ディジタル信号の各パケットに付加されて記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求項１５記載のディジタル信号再生装置。

【請求項１７】所定長のディジタル信号に、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第１の誤り訂正符号を付加し、さらにｎ（ｎは１以上の整数）セクタ単位で第２の誤り訂正符号を付加し、前記第２の誤り訂正符号にも第１の誤り訂正符号を付加して、記録媒体上に記録されている前記ディジタル信号を再生するディジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするディジタル信号再生装置。

【請求項１８】少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力され、所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。

【請求項１９】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報を、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記更新された鍵に切り換える手段を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。

【請求項２０】前記再生手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で更新されているところの、前記鍵情報を、再生していく機能を備えたことを特徴とする請求項１９記載のディジタル信号再生装置。

【請求項２１】前記再生手段は、前記記録媒体上の所定の領域に記録されている、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を再生する機能を備え、前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。

【請求項２２】前記再生手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で切り換えられているところの、前記暗号フラグを、再生していく機能を備えたことを特徴とする請求項２１記載のディジタル信号再生装置。

【請求項２３】ディジタル信号が記録されているディジタル信号記録媒体において、

鍵情報に所定の演算を行って得られた鍵で暗号化された前記ディジタル信号と共に、前記鍵情報が、所定の領域に記録されていることを特徴とするディジタル信号記録媒体。

【請求項２４】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項２３記載のディジタル信号記録媒体。

【請求項２５】前記鍵情報が所定間隔で更新され、所定の領域に記録されていることを特徴とする請求項２３記載のディジタル信号記録媒体。

【請求項２６】ディジタル信号を変換するための複数種類の鍵を発生する鍵発生手段と、

前記鍵を用いてディジタル信号を変換し、変換後の変換ディジタル信号を出力する変換手段と、

前記鍵および前記変換ディジタル信号を記録媒体に記録する記録手段と、

を備えてなることを特徴とするディジタル信号記録装置。

5

【請求項２７】複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された媒体が用いられ、
前記変換ディジタル信号および前記鍵を前記媒体から再生し、出力する再生手段と、
前記再生手段からの出力が入力され、前記変換ディジタル信号を前記鍵を用いて復号変換する復号変換手段と、を備えてなるディジタル信号再生装置
【請求項２８】複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタル信号を記録媒体に記録再生するディジタル信号記録装置、再生装置、および記録媒体に関し、特に記録媒体上のディジタル信号の著作権を保護する機能を有するディジタル信号記録装置、再生装置、および記録媒体に関する。
【０００２】
【従来の技術】近年、ディジタル技術を用いた映像、音声等のデータ圧縮の研究が進み、これらデータの蓄積、伝送が容易にできるようになった。これに伴い、放送の分野においてもディジタル化が急速に進められている。
【０００３】例えば、アナログ映像信号、音声信号をＭＰＥＧ（Moving Picture Experts Group）規格を用いて高能率にディジタル圧縮符号化し、衛星や同軸ケーブルを通して放送するシステムが知られている。このディジタル放送を受信するための装置として、セットトップボックスと呼ばれるディジタル放送受信機がある。
【０００４】また、家庭用の映像信号、音声信号記録再生機器としては、磁気テープを用い、ディジタルＴＶ放送などのディジタル圧縮符号化された映像信号及び音声信号をディジタル信号のまま記録し再生できるディジタルＶＴＲの開発が進められている。
【０００５】このディジタル放送受信機とディジタルＶＴＲは、ディジタルインターフェースで接続され、受信したディジタル放送を高品質で保存可能となる。
【０００６】さらに、光ディスクやハードディスクを用い、映像信号及び音声信号を記録し再生する装置の開発が進められている。
【０００７】複数の情報が多重されて伝送されてくるディジタル信号を受信して所望の番組を選択する技術が、日本特開平８－５６３５０号に述べられている。また、回転磁気ヘッドを用いたディジタルＶＴＲについては、例えば、日本特開平５－１７４４９６号に記載されている。
【０００８】さらに、ディジタル放送受信機とディジタルＶＴＲをディジタルインターフェースで接続したディジタル放送記録システムについて、アイイーイーイートランザクションス　オン　コンシューマー　エレクトロニクス、第４２巻３号、１９９６年８月、６１７～６２２頁（IEEE Transactions on Consumer Electronics,

6

Vol. 42, No. 3, August 1996, p617～622 「Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era」）に詳しく述べられている。
【０００９】
【発明が解決しようとする課題】しかしながら、ディジタル放送等をディジタルＶＴＲ等で記録した、記録媒体上のディジタル信号の著作権の防衛については何ら考慮されていない。
【００１０】本発明の目的は、記録媒体上のディジタル信号の著作権を保護することにある。
【００１１】
【課題を解決するための手段】本発明は、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。
【００１２】
【発明の実施の形態】以下、本発明の実施例を図面を用いて説明する。
【００１３】図１はディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。２００はディジタル信号記録再生装置、２０１はディジタル放送受信装置、２０２はアンテナ、２０７は受像機である。また、２０３はチューナ、２０４は選択回路、２０５は復号回路、２０６はインターフェース回路、２０８はディジタル放送受信機２０１の動作の制御を行う制御回路である。ここで、ディジタル放送受信機２０１とディジタル信号記録再生装置２００は別体の構成で表示されているが、一体の構成となっていてもよい。
【００１４】図２は図１のディジタル信号記録再生装置２００の構成図である。図２は記録再生兼用の装置であるが、記録と再生が独立していても同様である。１００は回転ヘッド、１０１はキャプスタン、１０２ａは記録時の記録信号の生成等を行う記録信号処理回路、１０２ｂは再生時の再生信号の復調等を行う再生信号処理回路、１０４は記録再生モード等の制御を行う、例えば、マイクロプロセッサのような制御回路、１０５は回転ヘッド１００の回転等の基準となるタイミング信号を生成するタイミング生成回路、１０６は回転ヘッド及びテープの送り速度を制御するサーボ回路、１０７は記録信号の入力または再生信号の出力を行う入出力回路、１０９は記録時のタイミングを制御するタイミング制御回路、１１０は基準クロックを生成する発振回路、１１１はテープ、１１２はアナログ映像信号の記録再生回路、１１５はディジタル信号記録時のデータ暗号回路、１１６はディジタル信号再生時のデータ復号回路、１１７は、ディジタル情報を暗号あるいは復号する際にデータ暗号回

路１１５あるいはデータ復号回路１１６に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、１１８はディジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるブロック鍵を発生するブロック鍵発生器、１１９は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

【００１５】ディジタル映像圧縮信号は、パケット形式のデータで、複数チャンネルの信号が時分割多重されて伝送される。図１において、アンテナ２０２で受信されたディジタル放送信号は、チューナ２０３で復調され、その後、選択回路２０４で必要なディジタル圧縮映像信号が選択される。選択されたディジタル圧縮映像信号は、復号回路２０５で通常の映像信号に復号されて、受像機２０７に出力される。また、受信信号にスクランブル等の処理が行われているときは、選択回路２０４においてそれを解除した後に、復号処理が行なわれる。受信したディジタル放送信号の記録を行うときは、選択回路２０４において記録するディジタル圧縮映像信号及びそれに関連した情報が選択され、インターフェース回路２０６を介してディジタル信号記録再生装置２００の入出力端子１０８より、ディジタル信号記録装置２００に入力され、記録される。また、記録したディジタル放送信号の再生を行うときは、ディジタル信号記録再生装置２００で再生されたディジタル圧縮映像信号等が、入出力端子１０８よりインターフェース回路２０６に出力される。インターフェース回路２０６に入力されたディジタル圧縮映像信号等は、選択回路２０４、復号回路２０５により、通常の受信時と同様の処理を行って、受像機２０７に出力する。

【００１６】図１のディジタル信号記録再生装置２００の構成を示す図２において、記録時には、入出力端子１０８より入力されたパケットデータの一部が、入出力回路１０７を介して制御回路１０４に入力される。制御回路１０４では、パケットデータに付加されている情報あるいはパケットデータとは別に送られてきた情報によりパケットデータの種類等を検出し、検出結果によって記録モードを判断し、記録信号処理回路１０２ａ及びサーボ回路１０６の動作モードを設定する。次に入出力回路１０７は、記録するパケットデータをデータ暗号回路１１５に出力する。データ暗号回路１１５では、デバイス鍵発生器１１７およびブロック鍵発生器１１８により発生される鍵をもとに制御回路１０４において生成されるデータ鍵によって、入力されたパケットデータを暗号化し、これを入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５からの時間情報をもとに、入力されたパケットデータにタイムスタンプを施し、これを記録信号処理回路１０２ａに出力する。記録信号処理回路１０２ａでは、制御回路１０４で判断された記録モードに応じて、誤り訂正符号、ＩＤ

情報、サブコード、暗号化に使用したブロック鍵情報等を含む記録データの生成を行い且つ記録信号を生成して、回転ヘッド１００によりテープ１１１に記録する。

【００１７】再生時には、まず任意の再生モードで再生動作を行い、再生信号処理回路１０２ｂでＩＤ情報を検出する。そして、制御回路１０４でどのモードで記録されたかを判断し、再生信号処理回路１０２ｂ及びサーボ回路１０６の動作モードを再設定して再生を行う。再生信号処理回路１０２ｂでは、回転ヘッド１００より再生された再生信号より、同期信号の検出、誤り検出訂正、ブロック鍵情報等の取得を行い、パケットデータを再生して入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５で生成されたタイミングを基準としてタイムスタンプを取り除いたパケットデータをデータ復号回路１１６に出力する。データ復号回路１１６では、デバイス鍵発生器１１７により発生される鍵、および再生によって得られたブロック鍵をもとに、制御回路１０４において生成されるデータ鍵によって復号して、入出力回路１０７に出力する。

【００１８】記録時には、入出力端子１０８より入力された記録データのレートを基準としてタイミング制御回路１０９により記録再生装置の動作タイミングを制御し、再生時には、発振回路１１０により発振されたクロックを動作基準として動作する。

【００１９】図３はディジタル映像圧縮信号のパケットの構成図である。１パケットは固定長、例えば、１８８バイトで構成されており、４バイトのパケットヘッダ３０６と、１８４バイトのパケット情報３０７により構成されている。ディジタル圧縮映像信号は、パケット情報３０７の領域に配置される。また、パケットヘッダ３０７はパケット情報の種類等の情報により構成される。

【００２０】図４は図３のパケットヘッダ３０６の構成図である。５０１はパケットの先頭を示す同期バイト、５０２は誤りの有無を示す誤り表示、５０３はユニットの開始を示すユニット開始表示、５０４はパケットの重要度を示すパケットプライオリティ、５０５はパケットの種類を示すパケットＩＤ、５０６はスクランブルの有無を示すスクランブル制御、５０７は追加情報の有無及びパケット情報の有無を示すアダプテーションフィールド制御、５０８はパケット単位でカウントアップされる巡回カウンタである。

【００２１】図５はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。７１は図３のパケットである。通常、上記映像信号に音声信号、プログラムに関する情報等が付加され、複数チャンネルのプログラムが時分割多重されて伝送される。

【００２２】図５（ａ）は、３チャンネルのプログラムを多重した例であり、Ｖ１、Ｖ２、Ｖ３はそれぞれのチャンネルの映像信号、Ａ１、Ａ２、Ａ３はそれぞれのチャンネルの音声信号のパケットである。なお、映像また

は音声は、一つのチャンネルに複数の映像または音声で構成されている場合もある。Ｐ０、Ｐ１、Ｐ２、Ｐ３はプログラムに関する情報である。それぞれのパケットは、異なるパケットＩＤ５０５が割り当てられており、これによりパケットの内容を識別することができる。

【００２３】Ｐ０は、図５（ａ）の伝送信号全体に関する情報であり、それぞれのプログラムにどのパケットＩＤが割り当てられているかを認識するためのプログラムアソシエーションテーブル、番組ガイド情報等のパケットが時分割多重されて伝送される。Ｐ１、Ｐ２、Ｐ３は、それぞれのプログラムに関する情報であり、そのチャンネルの映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識するためのプログラムマップテーブル、スクランブル情報等のパケットが時分割多重されて伝送される。通常、プログラムアソシエーションテーブルのパケットＩＤは決まった値、例えば０が割り当てられている。

【００２４】受信時には、まずプログラムアソシエーションテーブルによって受信したいプログラムのプログラムマップテーブルにどのパケットＩＤが割り当てられているかを認識し、次に、受信したいプログラムのプログラムマップテーブルによって映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識する。そして、映像パケットおよび音声パケットを抽出してディジタル圧縮データの復号を行う。また、同時にプログラムクロックリファレンスを抽出し、これによってディジタル圧縮データの復号回路の復号タイミングが符号化時のタイミングと同期するように復号回路の動作を制御する。

【００２５】ＣＲは、ディジタル圧縮データの復号時の同期をとるためのプログラムクロックリファレンス情報である。

【００２６】もちろん、多重するチャンネル数は３チャンネル以外、例えば４チャンネルでもよいし、また、これ以外の情報を多重してもよい。

【００２７】図５（ｂ）は、図５（ａ）から第１のチャンネルの情報およびそれに関連したプログラム情報のみを選択したものである。第１のチャンネルを記録する場合には、この情報をディジタル放送受信機２０１から記録再生装置２００に出力する。もちろん、これ以外の情報を含めて記録してもよいし、また、再生時の処理をやりやすくするために、パケットの情報の一部を変更してもよい。例えば、プログラムアソシエーションテーブルの情報を記録するプログラムのみの情報に変更すれば、再生時にチャンネルの選択が不要になる。

【００２８】図６は図２のデータ暗号回路１１５の構成図である。１１５１はパケットデータ入力端子、１１５７はパケットデータ出力端子、１１５３ａ、１１５３ｂはデータ鍵入力端子、１１５３ｃはデータ鍵選択信号入力端子、１１５３ｄは、処理モード選択信号入力端子、

１１５２、１１５６はブロック処理回路、１１５４は鍵スケジュール回路、１１５５は暗号器、１１５８ａ，１１５８ｂはデータ鍵レジスタ、１１５９はデータ鍵セレクタである。データ暗号回路１１５は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で暗号化して出力する。この際、このデータ鍵をある時間間隔で変更していくことにより、テープ上に記録されるパケットデータの安全性を高めることができる。

【００２９】暗号器１１５５は、例えば、伝送中にビット誤り等のエラーが発生しても、そのエラーが後続のデータに影響を与えない、すなわちエラー伝播がないように、複数ビットで構成されるブロックを単位として暗号処理を簡単な回路構成で実現できるブロック暗号を用いる。

【００３０】入力端子１１５１から入力されたパケットデータは、まず、ブロック処理回路１１５２において、複数ビットからなるブロックＰに区切られる。例えば１ブロックを６４ビットとする。各ブロックは、暗号器１１５５において順次暗号化され、その結果ブロックＣを出力し、ブロック処理回路１１５６において、今度はブロックをパケットデータの形式に戻して出力端子１１５７へ出力する。ここで、暗号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１５３ａおよび１１５３ｂから入力され、データ鍵レジスタ１１５８ａ、１１５８ｂに記憶される。例えば、データ鍵レジスタ１１５８ａには、現在のデータ鍵を、データ鍵レジスタ１１５８ｂには次に切り換えるデータ鍵を記録させる。

【００３１】また、データ鍵選択信号入力端子１１５３ｃからは、制御回路１０４より、データ鍵レジスタ１１５８ａ、１１５８ｂのどちらのデータ鍵を選択するかを示す信号が入力され、データ鍵セレクタ１１５９により、選択されたデータ鍵が出力される。ここでは、例えば鍵レジスタ１１５８ａのデータ鍵が選択されているものとする。選択されたデータ鍵は、スケジュール回路１１５４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１５５に供給される。例えば、データ鍵の長さ５６ビット、サブ鍵の長さが、それぞれ３２ビットとし、データ鍵の上位３２ビットをＫＡに割り当て、データ鍵の上位３２ビットと下位３２ビットの加算値をＫＢに割り当てる。

【００３２】ここで、データ鍵を変更する場合には、制御回路１０４より、データ鍵レジスタ１１５８ｂを出力するようデータ鍵選択信号入力端子１１５３ｃから信号が入力される。データ鍵セレクタは、一つのパケットデータのブロック全ての暗号化が終了するまでは、その選択出力を切り換えず、次のパケットデータとの間で切り換えるよう制御する。

【００３３】その他、例えば、暗号器１１５５の出力と、暗号器１１５５の入力を排他的論理和をとり、ブロ

ック単位でフィードバックをかけることで、暗号強度を増す方法もある。

【００３４】図７は図６の暗号器１１５５の構成図である。同図中、５５１、５５２、５５３、５５４は暗号処理部、Ｐａ、Ｐｂは入力ブロックデータＰの上位および下位ビット、Ｃａ、Ｃｂは暗号化されたデータ、ＫＡ、ＫＢは、サブ鍵である。同図に示すように、例えば入力された６４ビットのブロックＰを、その上位３２ビットＰａと下位３２ビットＰｂに分離する。そのＰａ、Ｐｂは、暗号処理部５５１において、排他的論理和（５５１１）、ビットシフトおよび加算演算（５５１２、５５１３、５５１５：Ａ＜＜＜ｐは、Ａをｐビット左方向に循環ビットシフトすることを表す）、加算演算（５５１４、５５１６）を行い、その結果を暗号処理部５５１と同様の処理を行う後続の暗号処理部５５２、５５３、さらに図示しない暗号処理部に入力して複数段繰り返し演算を行い、最終段の暗号処理部５５４により出力されたデータＣａ、Ｃｂより、暗号化されたブロックＣを得る。

【００３５】以上は、図２、図７のデータ暗号回路１１５について説明したが、図２のデータ復号回路１１６では、暗号器１１５５の逆の流れで演算していくことにより、暗号化されたブロックを復号することができる。ただし、図７の演算５５１６は、減算処理とする。また、当然、サブ鍵ＫＡ、ＫＢは、暗号時と同一の鍵を用いなければならない。

【００３６】その他、記録するパケットデータを保護する必要が無い場合、例えば記録する番組が自由にコピーしてもよいよう許可されている場合、パケットデータを暗号化しないで、そのままテープ上に記録する場合がある。これは例えば、データ暗号回路１１５、データ復号回路１１６を、入力パケットの暗号・復号の機能と、なにもしないで通過させる機能とを切り換えることで実現できる。図２、図６のデータ暗号回路１１５において、図６の処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号により、図７の演算５５１６への入力Ｘ５を、図示していないが、零に固定することで、暗号、復号処理を行わずに、ブロックを通過させることが出来る。この方法によれば、入力パケットの通過遅延時間を一定に保ったまま、動作を切り換えることができる。また、図示しないが、他の方法としては、入力端子１１５１から入力されたパケットデータを、ブロック処理回路１１５２、暗号器１１５５、ブロック処理回路１１５６を介さず、出力端子１１５７に出力するか、ブロック処理回路１１５６から出力されるパケットデータを出力端子１１５７に出力するかを切り換える切り換え回路を出力端子１１５７の前段に設け、処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号をその切り換え回路に入力して、ブロック処理回路１１５６から出力されるパケットデータか、入力端子１１５７に入力されたパケットデータかを切り換える方法もある。これらの方法は、図２、図１９のデータ復号回路１１６においても前述と同様の構成で実現できる。

【００３７】図８は図２のデータ暗号回路１１５、データ復号回路１１６に供給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。デバイス鍵発生器１１７は、例えば９６ビットのあらかじめ定められた固定の鍵情報を記憶している。ブロック鍵発生器１１８は、例えば図２の制御回路１０４からの司令１１８１により、９６ビットの乱数を発生させる乱数発生器である。１２０は９６ビットの排他的論理和演算器、１２１はハッシュ関数演算器である。図８（ａ）では、ブロック鍵とデバイス鍵は、排他的論理和演算器１２０で排他的論理和がとられ、ハッシュ関数演算器１２１にてハッシュ演算がなされ、その結果のうちの選択された５６ビットが、データ鍵として図２のデータ暗号回路１１５に供給される。ハッシュ関数は、その出力結果から、入力データが類推困難な関数であり、データ鍵から、秘密情報であるブロック鍵、デバイス鍵が求められない。

【００３８】また、図２の制御回路１０４からの司令１１８１をある時間間隔で発生させ、上述の演算によるデータ鍵生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、記録媒体上のデータの安全性を高めることが可能となる。次に、ブロック鍵発生器１１８で発生されたブロック鍵（Ｋｒ）は、図２の記録信号処理回路１０２ａに送られ、テープ１１１上に記録される。

【００３９】再生時には、ブロック鍵発生器１１８の発生するブロック鍵の代わりに、テープ１１１上から再生されたブロック鍵（Ｋｐ）を用いて、上記と同様の演算を行い、データ鍵を得、図２のデータ復号回路１１６に供給される。

【００４０】図８（ｂ）は、テープ１１１上に記録する鍵情報Ｋｒとして、ブロック鍵をデバイス鍵で排他的論理和演算したものを用いる例である。この場合、ハッシュ関数演算器にはブロック鍵そのものが入力される。再生時には、図８（ａ）中のブロック鍵の代わりに、テープ１１１上から再生されたＫｐを用いて、上記と同様の演算を行い、データ鍵を得、データ復号回路１１６に供給される。

【００４１】次に、テープへの記録方法について述べる。

【００４２】図９は、１トラックの記録パターンである。３は時間情報、プログラム情報等のサブコードを記録するサブコード記録領域、７はディジタル圧縮映像信号を記録するデータ記録領域、２及び６はそれぞれの記録領域のプリアンブル、４及び８はそれぞれの記録領域のポストアンブル、５はそれぞれの記録領域の間のギャ

ップ、１及び９はトラック端のマージンである。このように、各記録領域にポストアンブル、プリアンブル及びギャップを設けておくことにより、それぞれの領域を独立にアフレコを行うことができる。もちろん、記録領域７にはディジタル圧縮映像信号以外のディジタル信号を記録してもよい。データ記録領域７は、複数のブロック（前述の暗号化の小単位であるブロックとは異なる）により構成されている。

【００４３】図１０は図９のデータ記録領域７のブロックの構成図である。２０は同期信号、２１はＩＤ情報、２２はデータ、２３は第１の誤り検出訂正のためのパリティ（Ｃ１パリティ）である。例えば、同期信号２０は２バイト、ＩＤ情報２１は３バイト、データ２２は９９バイト、パリティ２３は８バイトで構成されており、１ブロックは１１２バイトで構成されている。

【００４４】図１１は図１０のＩＤ情報２１の構成図である。３１はグループ番号、３２はトラックアドレス、３３は１トラック内のブロックアドレス、３５はグループ番号３１、トラックアドレス３２及びブロックアドレス３３の誤りを検出するためのパリティである。ブロックアドレス３３は、各記録領域でのブロックの識別を行うためのアドレスである。例えば、図９のデータ記録領域７では０～３３５とする。トラックアドレス３２は、トラックの識別を行うためのアドレスであり、例えば、１トラックまたは２トラック単位でアドレスを変化させ、ｎトラックを識別することが出来る。例えば、０～５または０～２とすることにより、６トラックを識別することができる。図１１のグループ番号３１は、例えば、トラックアドレス３２で識別する６トラック単位で変化させ、０～１５とすることにより、９６トラックを識別することができる。トラックアドレス３２は、後述する第２の誤り訂正符号の周期と同期させておけば、記録時の処理及び再生時の識別を容易にすることができる。

【００４５】図１２は図９のデータ記録領域７の１トラック分のデータの構成図である。なお、図１０に図示の同期信号２０およびＩＤ情報２１は省略してある。データ記録領域７は、例えば、３３６ブロックで構成されており、最初の３０６ブロックにデータ４１を、次の３０ブロックに第２の誤り訂正符号（Ｃ２パリティ）４３を記録する。Ｃ２パリティ４３は、ｎトラック単位、例えば６トラック単位で構成されている。６トラック単位でみると、データは３０６ブロック×６トラックのデータであり、そのデータを１８分割して、それぞれの１０２ブロックに、１０ブロックのＣ２パリティを付加する。誤り訂正符号は、例えばリードソロモン符号を用いればよい。各ブロック９９バイトのデータは、３バイトのヘッダ４４と９６バイトのデータ４１により構成されている。

【００４６】図１３は、１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、図１２のデータ４１に記録する時の１パケットのブロックの構成例である。この場合には、４バイトの時間情報２５を付加して１９２バイトとし、２ブロックに１パケットを記録する。時間情報２５は、パケットの伝送された時間の情報である。すなわち、パケットの先頭が伝送された時の時間またはパケット間の間隔を基準クロックでカウントし、そのカウント値をパケットデータと共に記録しておき、再生時にその情報を基にしてパケット間の間隔を設定することにより、伝送された時と同一の形でデータを出力することができる。

【００４７】図１４は図１２のデータ記録領域７のヘッダ４４の構成図である。ヘッダ４４は、フォーマット情報４５、ブロック情報４６および付加情報４７により構成される。フォーマット情報４５、およびブロック情報４６には、記録に関する様々な記録情報が、また付加情報４７には、その他補助的な情報が記録される。

【００４８】フォーマット情報４５は、記録フォーマットに関する情報であり、記録モード（標準速モードその他の識別）、取り扱うパケットデータの種類、記録されているパケットデータがコピー可能か否か等を示すコピー制限情報等が格納され、複数のブロックで、１つの情報を構成する。例えば１２ブロックの１２バイトで１つの情報を構成している。そして、この情報を複数回繰り返し多重記録することにより、再生時の検出能力を向上させている。ここに、前述の鍵情報等をも記録しておくことが可能である。

【００４９】ブロック情報４６は、データ記録領域４１に記録されるデータの種類を識別するための情報である。ここには、高速可変速再生用データの有無、種類（どの速度に対応した高速可変速再生用データであるか）等を記録しておく。ここに、前述の鍵情報等をも記録しておくことも可能である。

【００５０】付加情報４７は、例えば、６ブロックの６バイトで一つの情報であるパックデータを構成し、最初の１バイトが情報の種類を表すアイテムコード、残りの５バイトをデータとすることにより、いろいろな種類のデータを記録することができる。例えばここに前述のブロック鍵等の鍵情報や、その他、記録時間等の情報や記録信号の種類等を記録しておくことができる。

【００５１】図１５は図１４の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

【００５２】パックデータの最初の１バイトには後続の情報が鍵情報であることを示すアイテム情報コードを格納する。

【００５３】２バイト目には、格納されている鍵の種類を示す情報（鍵シーケンス番号、鍵属性、鍵フラグ）を記録する。前述のように、ブロック鍵をある時間間隔で順次変更していくことで、記録媒体上のデータの安全性

を高めることができるので、例えば、このパックに格納されているブロック鍵が、現在のパケットデータの暗号化に用いられるブロック鍵か、次に用いるブロック鍵かを示す鍵属性情報を記録しておく。また、ブロック鍵が更新される度に反転する鍵フラグで、切り換えタイミングを記録する。この情報により再生時の鍵の切り換えをスムーズにする。また、鍵シーケンス番号には、一つのパックでブロック鍵が格納できない場合、後続のパックがあることを示す情報を格納する。例えばブロック鍵が９６ビットの場合、３つのパックに分割して格納し、それぞれの鍵シーケンス番号には、２、１、０を格納し、０が最終パックであることを示す。その他、全体のデータのサイズを格納しておき、残りの大きさを知る方法もある。

【００５４】３バイト目から６バイト目に、ブロック鍵を収納する。

【００５５】前述の図８（ｂ）の例では、鍵情報Ｋｒがブロック鍵の代わりに格納される。

【００５６】図１６はブロック鍵の格納方法を示す図である。この例は、各トラックのパックデータには、現在の鍵情報のみを記録する場合である。したがって、前述の鍵属性は、現在の鍵を示すのみの固定情報であり、記録しなくてもよい。同図中（１）は、９６ビットの現在のブロック鍵Ａ（Ａ０乃至Ａ１１）が３個のパックに分割して格納される状態を示す。通常、これらのパックは、データの信頼性の向上のため、一つのトラックにつき、複数回記録される。例えば、３個のパックをトラックの最初、半ば、最後のそれぞれの領域に記録する（計９個）ことで、磁気ヘッドの目詰まり等による、再生信号のバースト欠落の影響を軽減できる。また、３個のパックは必ずしも連続したパックとして記録する必要はなく、各パックの間に他の情報を格納したパックを挿入し、鍵情報を格納しているパックを分散して記録することで、鍵情報自身の保護も可能となり、さらに信頼性が向上する。同図（２）はブロック鍵がＢに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Ｂの鍵フラグは反転している。

【００５７】図１７はブロック鍵の他の格納方法を示す図である。図１７は、現在の鍵情報と共に、次に使用する鍵情報もあらかじめ発生させておき記録する方法である。ここで、鍵属性情報は、現在のパケットデータの暗号化に用いられるブロック鍵の場合“０”、次に用いるブロック鍵の場合“１”とする。また、ブロック鍵が更新される度に反転する鍵フラグは“０”と“１”を交互に繰り返す。

【００５８】同図中（１）は、９６ビットの現在のブロック鍵Ａが格納される状態を示す。（２）には、次のブロック鍵Ｂが格納される。この（１）および（２）が、同一のトラック内のブロックの付加情報エリアに記録される。（３）は、ブロック鍵がＢに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Ｂは、鍵属性情報“０”の現在の鍵に、また、鍵フラグも反転している。さらに（４）は、次に用いる鍵Ｃが格納される。（３）および（４）が、同一のトラック内のパックデータとしてトラックに記録される。

【００５９】ブロック鍵の更新タイミングを示す鍵フラグの格納場所としては、付加情報４７のパックに格納する以外に、前述の図１４に示したフォーマット情報４５、あるいはブロック情報４６に格納する方法もある。

【００６０】以上のように、鍵情報が、テープ上に記録されるが、ブロック鍵を切り換えるタイミングとしては、前述のＣ２パリティの付加の単位であるｎトラック（本実施例では６トラック）の区切り目とすることで、再生時に、Ｃ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【００６１】また、以上の例ではブロック鍵が更新されるタイミングを示す情報を鍵フラグとして記録したが、図２の記録信号処理回路１０２aにおいて、前述の図１１に示したトラックアドレス３２、あるいはグループ番号３１の値と、Ｃ２パリティの演算の周期および更新のタイミングを同期させることで、特に鍵フラグを記録しなくとも、再生時における鍵情報の更新のタイミングを、このトラックアドレス３２あるいはグループ番号３１の値で検出することも可能である。例えば、図２の記録信号処理回路１０２aにおいて、トラックアドレス３２が、トラック１本毎に０から５の値を繰り返し、その値０から５の６本のトラックを、前述のＣ２パリティの付加の単位とする。そして、値が５から０になるタイミングで、データ暗号回路１１５において、ブロック鍵を更新して、記録する。再生時においては、図２の再生信号処理回路１０２bにおいて、このトラックアドレス３２の値が５から０になるタイミングを検出し、データ復号回路１１６において、鍵を更新していけばよい。また、さらに長い周期で更新する場合には、例えば、グループ番号３１を用いて、トラックアドレス３２の値が５から０になる際に、グループ番号３１を１増加させ、０から１５の値を繰り返すようにすることで、９６トラックの単位で、しかもＣ２パリティの付加の単位の区切り目の、更新のタイミングを検出することが可能となる。

【００６２】図１８は図１３の時間情報２５（４バイト＝３２ビット）の具体的構成例であり、鍵フラグ、暗号フラグ格納の他の方法を示したものである。ここでは、例えば、時間情報２５１としては、２２ビットの情報であり、２５２は前述の鍵フラグ（１ビット）、２５３は、後続のパケットデータが暗号化されているかどうかを示す暗号フラグ（１ビット）である。記録時には、図２の入出力制御回路１１９は、タイムスタンプである時間情報２５１とともに、暗号フラグ２５３に、後続のパケットデータが暗号化されている場合には例えば“１”を、暗号化されていない場合には“０”を格納し、ま

た、鍵フラグ２５２には、後続のパケットデータに対応する前述の鍵情報を格納するパックデータの鍵フラグを格納する。再生時には、図２の入出力制御回路１１９において、記録時に付加した時間情報２５を取り除いてデータ復号回路１１６に出力するとともに、暗号フラグ２５３、鍵フラグ２５２をデータ復号回路１１６に供給し、データ復号回路１１６の動作を制御する。

【００６３】図１９は図２のデータ復号回路１１６の構成図である。１１６１はパケットデータ入力端子、１１６７はパケットデータ出力端子、１１６３ａ、１１６３ｂはデータ鍵入力端子、１１６３ｃはデータ鍵選択信号入力端子、１１６３ｄは、処理モード選択信号入力端子、１１６２、１１６６はブロック処理回路、１１６４は鍵スケジュール回路、１１６５は復号器、１１６８ａ，１１６８ｂはデータ鍵レジスタ、１１６９はデータ鍵セレクタである。データ復号回路１１６は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で復号化して出力する。

【００６４】復号器１１６５は、複数ビットで構成されるブロックを単位として復号処理を実現するブロック暗号を用いる。

【００６５】入力端子１１６１から入力されたパケットデータは、データ暗号回路１１５と同様に、複数ビットからなるブロックＣに区切られ、各ブロックは、復号器１１６５において順次復号化され、その結果ブロックＰを出力し、ブロック処理回路１１６６において、パケットデータの形式に戻して出力端子１１６７へ出力する。ここで、復号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１６３ａおよび１１６３ｂから入力され、データ鍵レジスタ１１６８ａ、１１６８ｂに記憶される。例えば、データ鍵レジスタ１１６８ａには、現在のデータ鍵を、データ鍵レジスタ１１６８ｂには次に切り換えるデータ鍵を記録させる。

【００６６】また、処理モード選択信号入力端子１１６３ｄからは、入出力制御回路１０９より検出した暗号フラグ２５３が入力され、復号器１１６５を復号動作のモードか、何もしないで通過させるモードかを決定する。さらに、データ鍵選択信号入力端子１１６３ｃからは、入出力制御回路１０９より検出した鍵フラグ２５２が入力され、データ鍵セレクタ１１６９により、選択されたデータ鍵が出力される。選択されたデータ鍵は、スケジュール回路１１６４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１６５に供給される。

【００６７】ここで、図２の入出力制御回路１１９で検出した、暗号フラグ、あるいは鍵フラグが変化すると、それに連動して、データ復号器１１６の動作モード、データ鍵の選択が行われる。

【００６８】以上のように、各パケットデータへ暗号フラグ、鍵フラグを付加することにより、パケットデータ単位での、暗号化の有無、鍵情報の判別、および復号処理が実現できる。

【００６９】その他、暗号化されているかどうかを示す暗号フラグの格納場所としては、図１５に示した鍵情報を格納するパックの２バイト目に格納する方法、あるいは前述の図１４に示したフォーマット情報４５、ブロック情報４６に格納する方法もある。

【００７０】暗号フラグをフォーマット情報４５、あるいはブロック情報４６等に格納することで、例えば暗号フラグが“１”を示す時、すなわちパケットデータが暗号化されている場合には、データ復号回路１１６の動作を復号動作とするとともに、付加情報４７の鍵情報を格納するパックから、鍵情報を取得するようにし、暗号フラグが“０”の場合は、データ復号回路１１６の動作を、復号しないでそのまま出力するようにすることで、パケットデータが暗号化されていない場合の制御動作の簡略化が図れる。また、暗号フラグを鍵情報を格納するパックに格納する方法では、暗号フラグが“０”、すなわちパケットデータが暗号化されていない場合は、そのパックの３バイト目以降のブロック鍵情報は格納されていない。

【００７１】その他、暗号フラグを用いずに、例えば、鍵情報を格納するパックの有無で暗号化されているかどうかを判別することもできる。

【００７２】図２０は図２の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。４００はメモリ回路、４０１は図２の制御回路１０４に従いメモリ回路４００を制御するアドレス等を生成するメモリ制御回路、４０２はＣ２パリティ演算回路、４０３はＣ１パリティ演算回路、４０４は前記制御回路１０４からの設定内容に従い記録時のＩＤ情報、サブコード生成、フォーマット情報、ブロック情報、鍵情報等の付加情報の付加、および再生時のＩＤ情報、サブコード、フォーマット情報、ブロック情報、鍵情報等の付加情報の取得等を行う付加情報処理回路、４０５は記録時の変調処理及び再生時の復調処理を行う変復調回路である。本実施例では、一例としてＣ２パリティ演算を行うために６トラックのデータを必要とするため、メモリ回路４００は少なくとも６トラック分のデータを蓄積する容量を備えるものとする。

【００７３】記録時には、端子４１１、４１３を介して図２の制御回路１０４により、記録状態に設定される。図２のデータ暗号回路１１５で暗号化されたパケットデータが端子４１０から入力され、メモリ制御回路４０１の制御信号に従いメモリ回路４００に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力されて、所定の演算が行われる。Ｃ２パリティ演算回路４０２で得られた演算結果は、メモリ回路４００に蓄積される。一方、端子４１３を介して図２の制

19

御回路１０４からの設定に従い、付加情報処理回路４０４で、入力された暗号化パケットデータの鍵に対応した鍵情報等のパックデータが生成され、メモリ回路４００に蓄積される。さらに前記した記録ブロックを構成するように、鍵情報等を含めメモリ回路４００から読みだされたデータは、Ｃ１パリティ演算回路４０３でＣ１パリティを付加され、変復調回路４０５に入力される。変復調回路４０５で所定の変調処理された信号は、端子４１４を介して出力され、図２の記録再生アンプ１１６、回転ヘッド１００を介してテープ１１１上に記録される。

【００７４】図２１はデータ記録開始時における信号処理のタイミングを示す図である。図２１（ａ）はデータ暗号化回路１１５から入力されるパケットデータ、図２１（ｂ）は、データ暗号化回路１１５が暗号化の際に用いたデータ鍵、図２１（ｃ）は、前述のＣ２パリテイ４３の６トラック単位構成にあわせて、図２０のＣ２パリティ演算回路４０２でのＣ２パリティ演算サイクル（本実施例では６トラック）を示し、図２１（ｄ）は回転ヘッド１００を介してテープ１１１に記録する記録信号を示している。図２１の実施例では、記録開始が設定される時間ｔ１より前にあらかじめブロック鍵Ａを生成し、データ鍵Ｋａを演算して、データ暗号化回路１１５に供給しておく。また、記録開始が設定される時間ｔ１より前は、記録信号処理回路１０２ａは入力信号に関らずパケット無しとみなして記録信号処理を行うように制御する。これにより、時間ｔ０に記録開始が設定されても、期間ｐ０のデータに対してのＣ２パリティの演算は可能となる。

【００７５】図２の制御回路１０４は、時間ｔ０で記録開始にした時の入力データのＣ２パリティ演算サイクルｓ０が終了して、前記第２の誤り訂正符号を構成するｎトラック（本実施例では６トラック）の先頭から記録信号を出力する（図２１（ｄ））ように制御する。また、データ鍵は、このＣ２パリティの演算サイクルで更新される。例えば、時間ｔ２より前にブロック鍵Ｂを生成し、データ鍵Ｋｂを演算してデータ暗号化回路１１５に供給しておき、時間ｔ２の時点でデータ暗号化回路１１５においてデータ鍵をＫｂに切り換える。通常、データ暗号化回路１１５は、その処理のため、パケットデータの入力から出力までの間に遅延時間が生じる。そこで、時間ｔ２からデータ暗号化回路１１５がパケットを暗号化処理することにより生じるデータ遅延時間分前の時点で、データ暗号化回路１１５に供給するデータ鍵をＫｂに切り換える。あるいは、データ鍵が切り換えられたパケットデータからは、次の演算サイクルの処理に先送りしてもよい。この実施例では、先頭部分に余分なデータが記録されるが、記録開始にする時間ｔ１のタイミングによらず、記録すべき信号に対しＣ２パリティを付加し、上記Ｃ２パリティ演算サイクル単位で記録できる。また、再生時において、先頭の余分なデータ部分は、パケット無しとみなして記録処理しているので、Ｃ２パリティ演算に用いられるだけで、出力されることはない。

20

【００７６】記録終了時には、前記記録再生信号処理回路１０２ａの、テープ１１１への記録動作を、複数トラックのデータを用いて演算するＣ２パリティの演算サイクル（本実施例では６トラック）完結で行うように前記制御回路１０４で制御する。この制御方式により、記録開始、記録終了の切換えタイミングによらず、テープ１１１上の記録データに全てＣ２パリティを付加し、Ｃ２パリティの演算サイクル単位で鍵情報が更新されパケットデータが暗号化されるので、再生時には、Ｃ２パリティ演算サイクル単位で再生でき、Ｃ２パリティ演算が可能となるので、鍵情報のデータ信頼性も向上する。

【００７７】図２２は図２のテープ１１１上の鍵情報を示す図である。同図中、１１１１から１１１７は、Ｃ２パリティ演算サイクルである６トラック単位で示した記録トラックである。この図の場合、記録トラック１１１１から１１１３までが、ブロック鍵Ａ、記録トラック１１１４から１１１６までがブロック鍵Ｂをもとに暗号化されたパケットデータ、およびそれらに対応した鍵情報であるパックデータが格納される。また、記録トラック１１１７は暗号化されずに記録されたトラックである。この図のように、暗号化されたトラックと、暗号化されていないトラックが同一のテープ上に混在することも可能である。鍵情報の更新は、例えば、４８トラック、９６トラック等、ｍ×ｎトラック毎（ｍは１以上の整数、ｎは本実施例では６）、あるいは一つの番組全体等考えられるが、鍵の切り換わり目、あるいは暗号化されたトラックと、暗号化されていないトラックとの境目は、Ｃ２パリティ演算サイクル（本実施例では６トラック）の区切り目である。

【００７８】以上、記録の際の動作について説明した。ここで、鍵情報をサブコード領域（図９の７）に記録することも可能であるが、鍵情報を、各ブロックのヘッダ（図１２の４４）の部分に格納し、各トラック上のデータ記憶領域（図９の７）に記録することで、アフレコ等による鍵情報のみの書き換えは困難となる。従って、鍵情報の消失を防ぐことができ、また、故意に鍵情報のみを改ざんして意図的に暗号通信を行うことはできない効果がある。

【００７９】次に、テープからの再生方法について述べる。

【００８０】図２０のディジタル記録再生信号処理回路１０２において、再生時は、端子４１１、４１３を介して図２の制御回路１０４によって、再生状態に設定される。前記テープ１１１から回転ヘッド１００で再生され、端子４１４から入力された再生信号は、変復調回路４０５で復調処理された後、Ｃ１パリティ演算回路４０３でＣ１パリティ演算を行い、誤り検出およびその訂正を行い、Ｃ１パリティ演算結果も一緒にメモリ回路４０

０に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ制御回路４０１の制御信号に従いメモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力される。Ｃ２パリティ演算回路４０２では、上記データで演算を行い、誤りの検出、訂正処理したデータおよびＣ２パリティ演算結果を、再びメモリ回路４００に蓄積する。

【００８１】図２のタイミング生成回路１０５から端子４１２を介して入力されるタイミング信号を基準として所定の順番にメモリ回路４００からデータを読みだし、前記Ｃ１パリティ、Ｃ２パリティの演算結果を参照し、誤りの無いデータのみを端子４１０から図２の入出力制御回路１１９に出力する。一方、付加情報処理回路４０４では、メモリ回路４００から読み出したデータから鍵情報やサブコード等を取得し、端子４１３を介して図２の制御回路１０４に送出する。その後、図８で示した演算、すなわち再生によって得られた鍵情報から、Ｋｐを取り出し、デバイス鍵発生器１１７からのデバイス鍵との排他的論理和をとって、ハッシュ関数１２１の演算を行い、データ鍵を得、図２のデータ復号回路１１６に出力する。このデータ鍵は、記録時に用いたデータ鍵と同一のものであり、データ復号回路１１６において、正しくもとのパケットデータを得ることができる。

【００８２】図２３は、本発明のデータ再生時における信号処理のタイミングを示す図である。図２３（ａ）は回転ヘッド１００を介してテープ１１１から再生される再生信号、図２３（ｂ）は上記Ｃ２パリティの演算サイクル（本実施例では６トラック）を示し、図２３（ｃ）は入出力制御回路１１９から出力されるパケットデータを示し、図２３（ｄ）は、図２のデータ復号回路１１６に供給されるデータ鍵を示している。付加情報処理回路４０４では、演算サイクルｓ３においては、このサイクルで用いられている鍵情報ＫｐＣが検出されている。このＫｐＣにより前述の演算で得られたデータ鍵Ｋｃが、例えば前述のデータ鍵レジスタ１１６３ａに記憶されており、データ鍵セレクタ１１６９も、データ鍵レジスタ１１６３ａのデータ鍵Ｋｃが出力されるように選択されている。

【００８３】次に、演算サイクルｓ４において、鍵情報ＫｐＤが用いられていることが検出されると、あらかじめ、データ鍵Ｋｄを前述の演算で求めておき、データ鍵レジスタ１１６３ｂに記憶させ、時間ｔ３のタイミングで、データ鍵セレクタ１１６９を制御してデータ鍵レジスタ１１６３ｂのデータ鍵Ｋｄに切り換える。以上の方法により、データ鍵を更新しながらの再生動作が可能となる。

【００８４】また、既に記録済みのテープに追加記録する場合、Ｃ２パリティの付加単位の区切り目から、記録を開始するようにすることで、追加記録直前のトラックの鍵情報のデータ信頼性を損なわずに、つなぎ記録が可能となる。

【００８５】その他、パケットデータが暗号化されているかいないかを区別する方法としては、図４で示した同期バイト５０１は、通常固定データであるので、例えば、再生信号処理回路１０２ｂにおいて、この同期バイトの検出を行い、検出できた場合は、図２のデータ復号回路１１６を入力されるパケットデータを何もしないで通過させる機能に切り換え、検出できなかった場合は、図２のデータ復号回路１１６を復号機能の動作に切り換え、付加情報エリア内の鍵情報を検出する動作を行うことで、記録時に、パケットデータを暗号化して記録されたトラックと、暗号化しないで記録したトラックとが混在するテープの場合にも、検出が可能となる。

【００８６】また、あらかじめ記録されているソフトテープについても、以上説明した方法で、ソフトテープの作成および再生が可能となり、テープ上のパケットデータの保護が実現できる。

【００８７】以上は、記録トラックに現在のブロック鍵が格納されている例を示したが、データ鍵の演算は、Ｃ２の一演算サイクル内で行わなければならない。Ｃ２の一演算サイクル内でデータ鍵の演算が間に合わない場合は、前述のように、記録トラック内に、現在のブロック鍵と、次のブロック鍵を記録しておくことで、あらかじめ、次のデータ鍵を求めておける。

【００８８】図２４は図１のディジタル信号記録再生装置２００の他の構成図である。同図中、１２１は、例えばＩＥＥＥ１３９４のような高速ディジタルバスインターフェース等のプロトコルを実現するディジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する、１２２は、ディジタルインターフェースバスである。１２３は、ディジタルインターフェース１２２上を伝送されるディジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してディジタルインターフェースバス１２２上に伝送し、あるいは受信したディジタルデータを復号化する。１２４は、マイクロプロセッサのような制御回路であり、ディジタルインターフェース回路１２１、暗号／復号回路１２３を制御する。

【００８９】記録時には、ディジタルインターフェースバス１２２上を伝送されてきた暗号化されたディジタルデータをディジタルインターフェース回路１２１において、所定のパケット処理を行い、暗号／復号回路１２３において、元のパケットデータに復号して、入出力回路１０７に出力する。その後、前述で説明したように、データ暗号回路１１５でパケットデータを暗号化し、テープ１１１上に記録する。再生時には、データ復号回路１１６において、再生したパケットデータを復号化して、入出力回路１０７から暗号／復号回路１２３に出力し、暗号／復号回路１２３において暗号化して、ディジタル

インターフェース回路１２１から、ディジタルインターフェースバス１２２に出力する。これによれば、テープ上のパケットデータ、ディジタルインターフェースバス上のパケットデータの双方の保護が実現できる。

【００９０】次に、光ディスクでの実施例を説明する。

【００９１】図２５は、ディスク上に記録されているファイルの構成図である。６０１はリードイン領域であり、各種パラメータが格納されている。６０２、６０３、…は、プログラム１領域、プログラム２領域、…であり、各プログラム領域には、それぞれ異なる番組等が格納されている。

【００９２】図２６は、一つのプログラム領域例えばプログラム１領域の構成図である。プログラム領域は複数のユニットで構成され、この各ユニットに、例えば、後述するディジタル圧縮映像信号の一つの単位であるシーケンスを一個格納する。

【００９３】図２７は、ディジタル圧縮映像信号のフレーム単位で圧縮されたイントラフレームデータと、前後のフレームのデータよりの予測を用いて差分情報のみの圧縮を行ったインターフレームデータの関係である。６２１はイントラフレーム、６２２はインターフレームである。ディジタル圧縮映像信号は、所定数のフレーム、例えば１５フレームを一つのシーケンスとし、その先頭はイントラフレーム６２１とし、残りのフレームはイントラフレーム６２１からの予測を用いて圧縮したインターフレーム６２２としている。もちろん、先頭以外にもイントラフレーム６２１を配置するようにしてもよい。

【００９４】図２８は、ディジタル圧縮映像信号の構成である。６２３はフレーム単位で付加されるピクチャヘッダ、６２４はシーケンス単位で付加されるシーケンスヘッダである。シーケンスヘッダ６２４は、同期信号及び伝送レート等の情報により構成される。ピクチャヘッダ６２３は、同期信号及びイントラフレームかインターフレームかの識別情報等により構成される。通常、各データの長さは情報量により変化する。前述の一つのユニットに１シーケンスが格納される。

【００９５】前述図２６の各ユニットは、複数のデータセクタにより構成される。

【００９６】図２９は各データセクタの構成図である。６３１はＩＤ情報で４バイト、６３２はＩＤ情報６３１の誤り検出訂正のためのパリティで２バイト、６３３は管理データで６バイト、６３４はユーザデータで２０４８バイト、６３５はユーザデータ６３４の誤り検出訂正のためのパリティで４バイトから構成される。このうちユーザーデータ６３４に、図２８で示したディジタル圧縮映像信号が、分割され格納される。その他、ディジタル圧縮音声圧縮信号も、分割されユーザーデータ６３４に格納される。前述の一つのユニットは、ディジタル圧縮映像信号、音声信号が、それぞれ格納されたデータセクタの集まりである。

【００９７】図３０は、ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。まず、データセクタが１７２バイトに区切られ、それに対し、１０バイトの第１の誤り検出訂正のためのパリティ６３７の一部（Ｃ１パリティパリティ６３７の一部）が付加される。さらにこのデータセクタをｎ個（例えば本実施例では１６個）集め、今度は行方向の１９２バイトに１６個の第２の誤り検出訂正のためのパリティ６３６（Ｃ２パリティ６３６）が付加される。得られたＣ２パリティ６３６にも１０バイトのＣ１パリティ６３７の一部が付加される。

【００９８】図３１は、光ディスクを記録媒体として用いたディジタル信号記録再生装置の構成図である。同図中、７０１は光ディスク、７０２は光ピックアップ、７０３ａは記録時の記録信号の生成等を行う記録信号処理回路、７０３ｂは再生時の再生信号の復調等を行う再生信号処理回路、７０４はマイクロプロセッサのような制御回路、７０５はスピンドルモータ、７０６は光ディスク７０１の回転速度および光ピックアップ７０２の位置、焦点を制御するサーボ回路、７０９は図６と同様の項構成のディジタル信号記録時のデータ暗号回路、７１０は図１９と同様の構成のディジタル信号再生時のデータ復号回路、７１１は、ディジタル信号を暗号あるいは復号する際にデータ暗号回路７０９あるいはデータ復号回路７１０に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、７１２はディジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるディスク鍵を発生するディスク鍵発生器、７１３はディジタル情報を暗号あるいは復号する際のデータ鍵のさらにもう一つのもとであるブロック鍵を発生するブロック鍵発生器、７１９はディジタルインターフェース回路、７２０は入出力端子である。

【００９９】記録時には、入出力端子７２０から、図２９のデータセクタのユーザデータ６３４の形式に区切られたディジタル圧縮映像信号等のディジタル信号が、ディジタルインタフェース回路７１９に入力される。入力されたディジタル信号は、データ暗号回路７０９において、デバイス鍵発生器７１１、ディスク鍵発生器７１２およびブロック鍵発生器７１３により発生される鍵をもとに制御回路７０４において生成されるデータ鍵によって、入力されたディジタル信号を暗号化し、これを記録信号処理回路７０３ａに出力する。記録信号処理回路７０３ａでは、入力されたユーザデータ形式のディジタル信号に、図２９のＩＤ６３１、パリティ６３２、管理データ６３３、およびパリティ６３５を付加し、データセクタの形式にする。次に、ｎ個のデータセクタを単位として（本実施例では１６個）、図３０のＣ１パリティ６３７、Ｃ２パリティ６３６を付加し、さらに図示しないが、所定の並べ替え、ヘッダを付加し、変調処理が施され、光ピックアップ７０２を介して光ディスク７０１上

に記録される。

【０１００】図３２は、データ暗号回路７０９に供給するデータ鍵の生成例であり、例えば、これらの生成は、図３１の制御回路７０４内にて行われる。デバイス鍵発生器７１１は、例えば９６ビットのあらかじめ定められた固定の鍵情報を記憶している。ディスク鍵発生器７１２、ブロック鍵発生器７１３は、例えば図３１の制御回路７０４からの司令７１２１、７１３１により９６ビットの乱数を発生させる乱数発生器である。７２１、７２２は９６ビットの排他的論理和演算器、７２３はハッシュ関数演算器である。まず、ブロック鍵は、ハッシュ関数演算器７２３にてハッシュ演算がなされ、その結果のうちの５６ビットが、データ鍵として図３１のデータ暗号回路７０９に供給される。また、９６ビットのブロック鍵は、９６ビットのディスク鍵と排他的論理和演算器７２２にて排他的論理和がとられ（以下鍵情報Ｋｒという）、図３１の記録信号処理回路７０３ａに送られ、光ディスク７０１上に記録される。さらに、ディスク鍵とデバイス鍵とが排他的論理和演算器７２１で排他的論理和がとられ（以下鍵情報ｋｄという）、図３１の記録信号処理回路７０３ａに送られ、光ピックアップ７０２を介して、光ディスク７０１上に記録される。

【０１０１】ここで、図３１の制御回路７０４からの司令７１３１を、ある時間間隔で発生させ、上述の演算によるデータ鍵の生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、光ディスク上のデータの安全性を高めることが可能となる。また、司令７１２１は、例えば一回の記録動作の際に一回発生させる。あるいは、空の光ディスクに最初に記録する際に一回だけ発生させてｋｄを記録し、次の記録動作からは、一旦光ディスク上の前述の鍵情報ｋｄを再生し、デバイス鍵と排他的論理和をとることで得られるディスク鍵を用いてブロック鍵と排他的論理和をとり鍵情報ｋｒを得る方法もある。さらに、ディスク鍵発生器７１２を用いずに、光ディスクの製造過程であらかじめ鍵情報ｋｄを記録しておき、記録動作の前にそのｋｄを再生し、ディスク鍵を得るという方法もある。鍵情報ｋｄは、例えば図２５のリードイン領域６０１に記録される。

【０１０２】再生の際には、まず鍵情報ｋｄを再生し、鍵情報ｋｄとデバイス鍵とを排他的論理和をとることでディスク鍵を得、さらに再生した鍵情報ｋｒと、得られたディスク鍵とを排他的論理和をとってブロック鍵を得、ハッシュ関数７２３の演算を行うことで、図３１のデータ復号回路７１０に入力するデータ鍵を得る。

【０１０３】図３１において、再生の際には、光ピックアップ７０２より再生された再生信号が再生信号処理回路７０３ｂに入力され、再生信号処理回路７０３ｂにおいて復調及び誤り検出訂正を行うとともに、図２９のユーザデータ６３４の形式のディジタル信号が、データ復号回路７１０に出力される。再生信号処理回路７０３ｂ

ではディスク鍵、ブロック鍵情報の再生も行い、制御回路７０４に送る。、制御回路７０４においては、前述のデータ鍵再生の演算を行ってデータ復号回路７１０に供給する。データ復号回路７１０において再生信号処理回路７０３ｂからのディジタル信号が復号され、ディジタルインターフェース回路７１９を介して入出力端子７２０から出力される。

【０１０４】なお、記録するディジタル信号を保護する必要がない場合は、暗号化しないでそのまま光ディスクに記録してもよい。

【０１０５】図３３は、図２９の管理データ６３３の構成図である。この管理データ６３３に、前述の鍵情報ｋｒを格納する。６３４１はこの管理データ６３３が格納されているデータセクタのユーザデータが暗号化されているかどうかを示す暗号フラグ、６３４２はこの管理データに格納されている鍵情報が有効か無効かを示すデータ有効フラグ、６３４３は鍵情報ｋｒが一つの管理データ６３３に格納できない場合、後続の管理データがあることを示す鍵シーケンス番号、６３４４は鍵情報ｋｒである。

【０１０６】図３４は、鍵情報ｋｒを図２９の管理データ６３３の領域に格納する方法を示す図である。この例では、図３０のＣ２パリティ６３６の付加単位である１６個のデータセクタ（データセクタ０～データセクタ０１５）の管理データを一つの単位として、前述の６４ビットの鍵情報を格納する。９６ビットの鍵情報ｋｒは３個の管理データにｋｒ０、ｋｒ１、ｋｒ２に分割され格納される。その際、暗号フラグ６３４１は暗号化されていることを示す１”が、データ有効フラグは有効であることを示す“１”が、また、鍵シーケンス番号６３４３は、３個の管理データに順に２、１、０を格納し、０が分割の最後であることを示す。これらが、１６個の管理データに繰り返し格納される。ただし、最後の管理データは、半端となるので、データ有効フラグは無効であることを示す“０”が、格納される。

【０１０７】以上のように、鍵情報が光ディスク上に記録される。この時、鍵情報は１６個またはその整数倍のデータセクタを単位として更新される。この鍵情報の更新は、６４データセクタ、１２８データセクタ等、ｍ×ｎデータセクタ毎（ｍは１以上の整数、ｎは本実施例では１６）等に行うことが考えられるが、鍵の切り換わり目、あるいは暗号化の有無の境目は、Ｃ２パリティの付加単位（本実施例では１６データセクタ）の区切り目である。このことにより、再生時にＣ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【０１０８】なお、記録信号処理回路７０３ａ、再生信号処理回路７０３ｂは、図２０のディジタル記録再生信号処理回路１０２の動作と同様の動作を行う。ただし、Ｃ２パリティの付加単位は、ｎデータセクタ単位（本実施例では１６データセクタ）となる。

【０１０９】図３５は、光ディスクを記録媒体として用いたディジタル信号記録再生装置の他の構成図である。本実施例では、図３に示したディジタル映像圧縮信号の固定長のパケットを光ディスク７０１に記録再生する場合の例である。図３５中、７１７は、例えばＩＥＥＥ１３９４のような高速ディジタルバスインターフェース等のプロトコルを実現するディジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する。７１８は、ディジタルインターフェースバスである。７１５はディジタルインターフェース７１８上を伝送されるディジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してディジタルインターフェースバス７１８上に伝送し、あるいは受信したディジタルデータを復号化する。７１６は、マイクロプロセッサのような制御回路であり、ディジタルインターフェース回路７１７、暗号／復号回路７１５を制御する。７０７はパケットデータをデータセクタのユーザデータに変換、あるいはユーザデータからパケットデータを取り出すセクタ変換回路、７０８は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

【０１１０】記録時には、ディジタルインターフェース回路７１７において、ディジタルインターフェースバス７１８上を伝送されてきた暗号化されたディジタルデータに所定のパケット処理を行い、暗号／復号回路７１５において、元のパケットデータに復号して、入出力回路７１４に出力する。その後、データ暗号回路７０９でパケットデータを暗号化し、入出力制御回路７０８において入力されたパケットデータにタイムスタンプを施し、セクタ変換回路７０７に出力する。セクタ変換回路７０７では、入力されたパケットデータを前述のデータセクタのユーザデータの形式に変換する。ユーザデータの形式に変換されたディジタル信号が、記録信号処理回路７０３ａ及び光ピックアップ７０２を介して、光ディスク７０１上に記録される。

【０１１１】したがって、光ディスク７０１上には、鍵情報に所定の演算を行って得られた鍵で暗号化された前記ディジタル信号と共に、前記鍵情報が、所定の領域に記録されている。また前記ディジタル信号は、所定長のパケット形式を有してなる。さらに、前記鍵情報が所定間隔で更新され、所定の領域に記録されている。またさらに、複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録されている。

【０１１２】再生時には、光ピックアップ７０２及び記録信号処理回路７０３ａを介して、セクタ変換回路７０７において、再生したユーザデータからパケットデータを取り出し、入出力制御回路７０８において記録時に付加されたタイムスタンプをもとに出力タイミングを制御しタイムスタンプが取り除かれたパケットデータが出力

される。さらに、データ復号回路７１０において、再生したパケットデータを復号化して、入出力回路７１４から暗号／復号回路７１５に出力し、暗号／復号回路７１５において暗号化して、ディジタルインターフェース回路７１７から、ディジタルインターフェースバス７１８に出力する。

【０１１３】図３６は、図３５のセクタ変換回路７０７によって変換された図２９のデータセクタのユーザデータ６３４に格納されるパケットデータの構成図である。ディジタル映像圧縮信号の固定長のパケットが複数個格納される。図３５の入出力制御回路７０８において、各パケット６４３，６４５、…には、例えば４バイトの時間情報６４２，６４４、…が付加される。データセクタが２０４８バイトの場合、時間情報が付加された１０個のパケットが格納可能である。時間情報が付加されたパケットは、連続して格納される必要はなく、途中に未使用領域があってもよい。また、パケットヘッダ６４１を付加することで、パケットの区切り目を容易に判別することができる。

【０１１４】本実施例においても、前述の鍵情報を切り換えるタイミング、あるいは暗号化の有無の境目としては、このＣ２パリティの付加単位であるｎデータセクタ（本実施例では１６データセクタ）の区切り目とすることで、再生時にＣ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【０１１５】図３７は、図３６の各時間情報６４２，６４４、…の構成図である。暗号フラグ６５１は、パケットが暗号化されているかどうかを示すフラグであり、鍵フラグは、このパケットが暗号化されている場合、どの鍵で暗号化されているかを示すフラグである。例えば、このフラグを２ビットとして、鍵が更新される度に０、１、２、３と１ずつ増加する値をとり、同様のフラグを図２９の管理データにも格納しておくことで、各パケット毎に対応する鍵を明示することができる。これらのフラグは、前述のパケットヘッダ６４１に格納してもよい。この方法によれば、パケット毎に任意に鍵を更新することが可能となる。

【０１１６】なお、以上の実施例では、磁気テープおよび光ディスクでの記録再生について説明したが、磁気ディスクや、半導体メモリ等、他のあらゆる記録媒体に記録再生する場合でも、同様に適用することができる。

【０１１７】上記半導体メモリの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えば半導体メモリの記録の一つの単位であるアドレスの区切り目で行うとよい。

【０１１８】また、本実施例は、本発明を、ディジタル信号を鍵により暗号化するシステムに適用したものである。しかし、本発明はこの実施例に限定されるものではなく、例えば、ディジタル信号がキーコードによりスクランブルされたりするシステムにも適用可能である。す

29

なわち、本発明は、少なくとも、ディジタル信号が元々のクリアな状態から変換されるように処理されるあらゆるシステムに対して適用可能なものである。

【０１１９】

【発明の効果】本発明によれば、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。以上により、再生の際には、前記所定の演算を施さない限り、前記鍵が得られないので、記録媒体上の鍵情報を得ても、それを用いて暗号化されたディジタル信号を復号することは困難であり、記録媒体上のディジタル信号の著作権を保護することができる。

【図面の簡単な説明】

【図１】本発明の実施例で、ディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。

【図２】図１のディジタル信号記録再生装置２００の構成図である。

【図３】ディジタル映像圧縮信号のパケットの構成図である。

【図４】図３のパケットヘッダ３０６の構成図である。

【図５】ディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。

【図６】図２のデータ暗号回路１１５の構成図である。

【図７】図６の暗号器１１５５の構成図である。

【図８】図２のデータ暗号回路１１５、データ復号回路１１６に供給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。

【図９】テープ１１１の１トラックの記録パターンを示す図である。

【図１０】図９のデータ記録領域７のブロックの構成図である。

【図１１】図１０のＩＤ情報２１の構成図である。

【図１２】図９のデータ記録領域７の１トラック分のデータの構成図である。

【図１３】１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、図１２のデータ４１に記録する時の１パケットのブロックの構成図である。

【図１４】図１２のデータ記録領域７のヘッダ４４の構成図である。

【図１５】図１４の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

【図１６】ブロック鍵の格納方法を示す図である。

【図１７】ブロック鍵の他の格納方法を示す図である。

【図１８】図１３の時間情報２５の具体的構成図である。

30

【図１９】図２のデータ復号回路１１６の構成図である。

【図２０】図２の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。

【図２１】データ記録開始時における信号処理のタイミングを示す図である。

【図２２】図２のテープ１１１上の鍵情報を示す図である。

【図２３】データ再生時における信号処理のタイミングを示す図である。

【図２４】図１のディジタル信号記録再生装置２００の他の構成図である。

【図２５】ディスク上に記録されているファイルの構成図である。

【図２６】一つのプログラム領域の構成図である。

【図２７】ディジタル圧縮映像信号のイントラフレームデータとインターフレームデータの関係を示す図である。

【図２８】ディジタル圧縮映像信号の構成図である。

【図２９】データセクタの構成図である。

【図３０】ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。

【図３１】光ディスクを記録媒体として用いたディジタル信号記録再生装置の構成図である。

【図３２】データ暗号回路７０９に供給するデータ鍵の生成例を示す図である。

【図３３】図２９の管理データ６３３の構成図である。

【図３４】鍵情報ｋｒを管理データ領域に格納する方法を示す図である。

【図３５】光ディスクを記録媒体として用いたディジタル信号記録再生装置の他の構成図である。

【図３６】図２９のデータセクタのユーザデータ６３４に格納されるパケットデータの構成図である。

【図３７】暗号フラグ等を前述の時間情報に付加する場合の時間情報の構成図である。

【符号の説明】

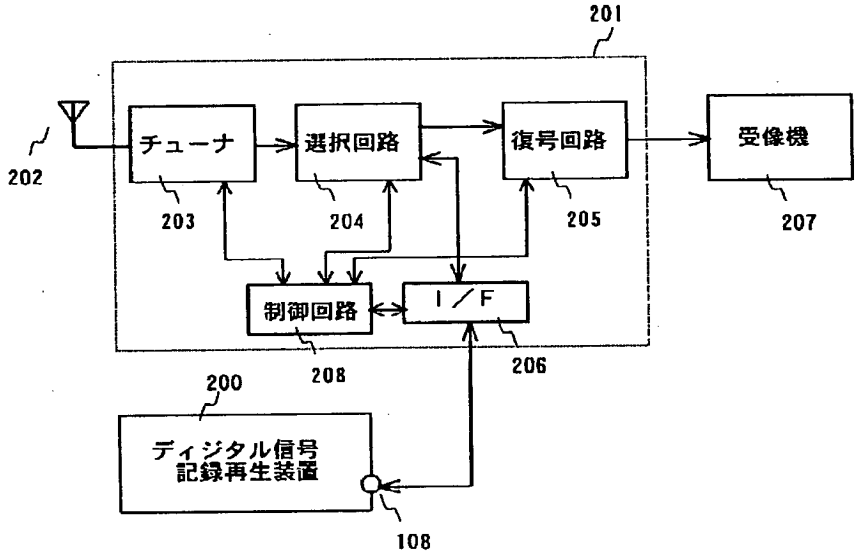
７…データ記録領域、２０…同期信号、２１…ＩＤ情報、２２…データ、２５…時間情報、３１…グループ番号、３２…トラックアドレス、３３…ブロックアドレス、４１…映像信号データ、４４…ヘッダ、４５…フォーマット情報、４６…ブロック情報、４７…付加情報、７１…パケット、１００…回転ヘッド、１０１…キャプスタン、１０２ａ…記録信号処理回路、１０２ｂ…再生信号処理回路、１０４…制御回路、１０５…タイミング生成回路、１０６…サーボ回路、１０７…入出力回路、１０９…タイミング制御回路、１１０…発振回路、１１５…データ暗号回路、１１６…データ復号回路、１１７…デバイス鍵発生器、１１８…ブロック鍵発生器、１１９…入出力制御回路、２００…ディジタル信号記録再生

装置、２０１…ディジタル放送受信機、２０３…チューナ、２０４…選択回路、２０５…復号回路、２０６…インターフェース回路、２０８…制御回路、１１５２…ブロック処理回路、１１５４…鍵スケジュール回路、１１５５…暗号器、１１５８…データ鍵レジスタ、１１５９…データ鍵セレクタ、１１６５…復号器、４００…メモリ回路、４０１…メモリ制御回路、４０２…Ｃ２パリティ演算回路、４０３…Ｃ１パリティ演算回路、４０４…付加情報処理回路、４０５…変復調回路、５５１…暗号

処理部。７０１…光ディスク、７０２…光ピックアップ、７０３ａ…記録信号処理回路、７０３ｂ…再生信号処理回路、７０４…制御回路、７０５…スピンドルモータ、７０６…サーボ回路、７０７…セクタ変換回路、７０８…入出力制御回路、７０９…データ暗号回路、７１０…データ復号回路、７１１…デバイス鍵発生器、７１２…ディスク鍵発生器、７１３…ブロック鍵発生器、７１９…ディジタルインターフェース回路。

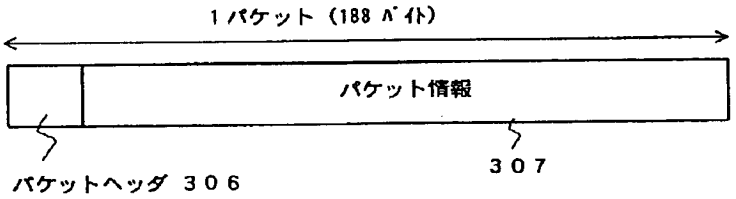
【図１】

図１



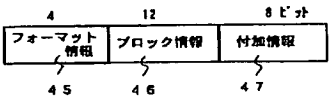
【図３】

図３



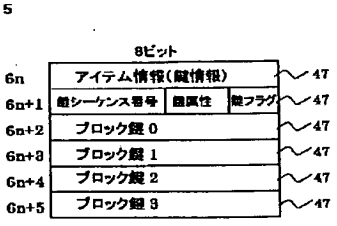
【図１４】

図１４



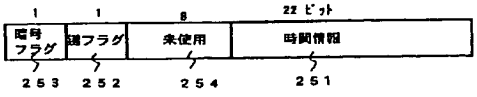
【図１５】

図１５



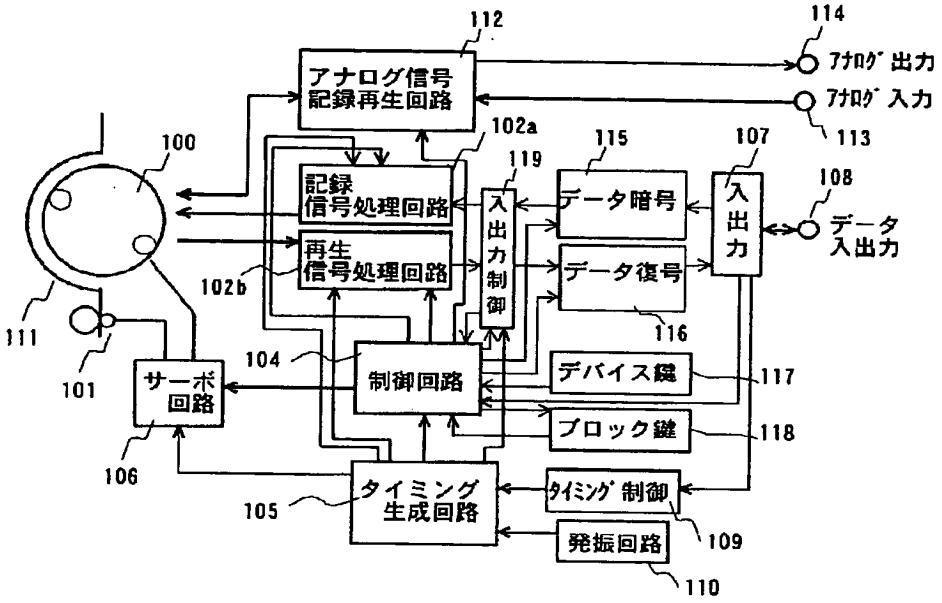
【図１８】

図１８



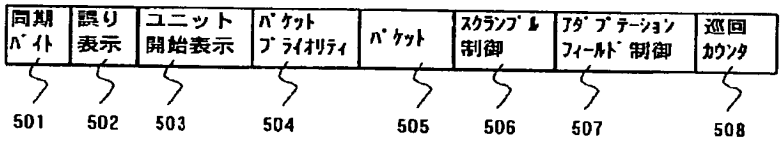
【図２】

図２



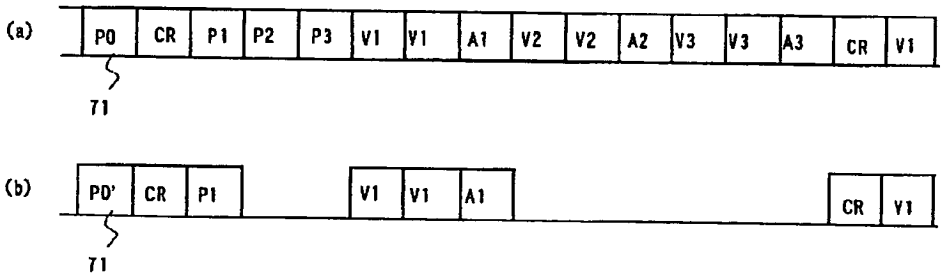
【図４】

図４



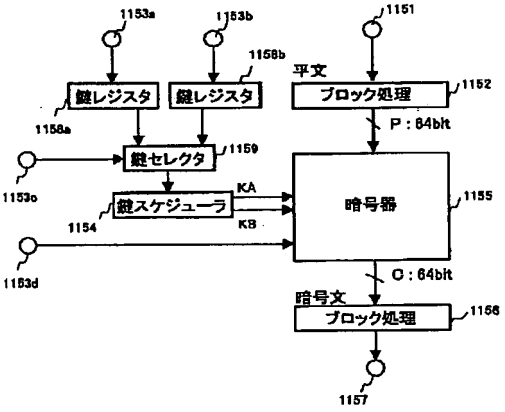
【図５】

図５



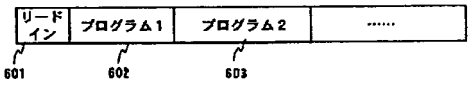
【図６】

図６



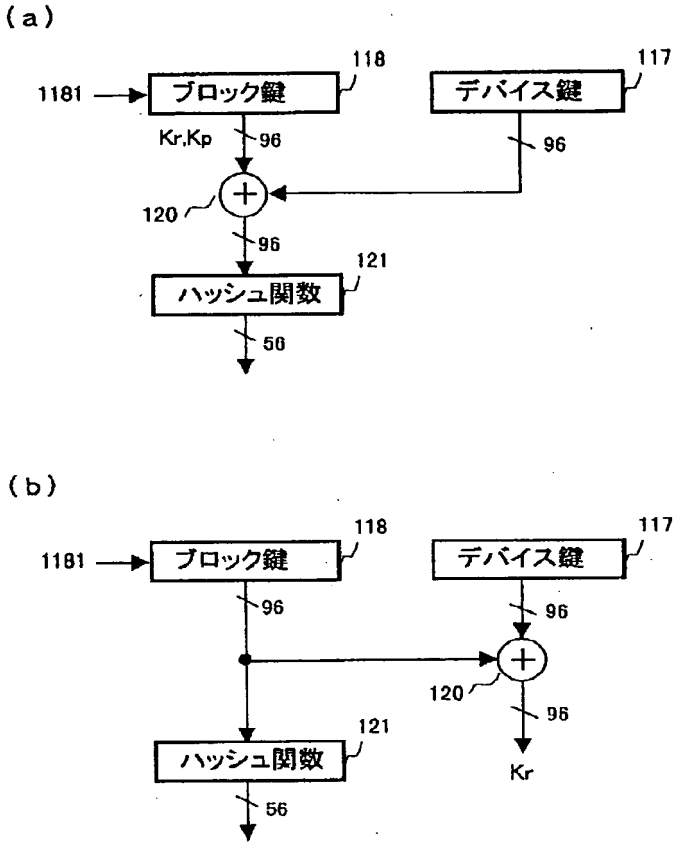
【図２５】

図２５



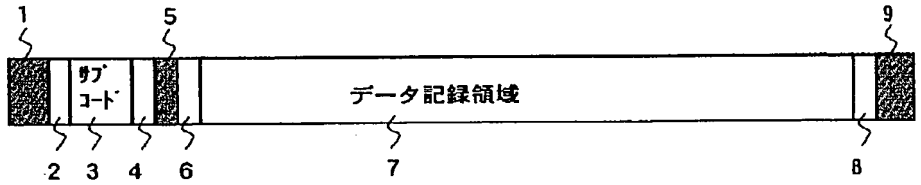
【図８】

図８



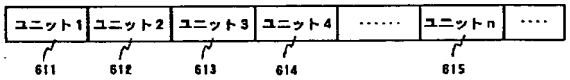
【図９】

図９



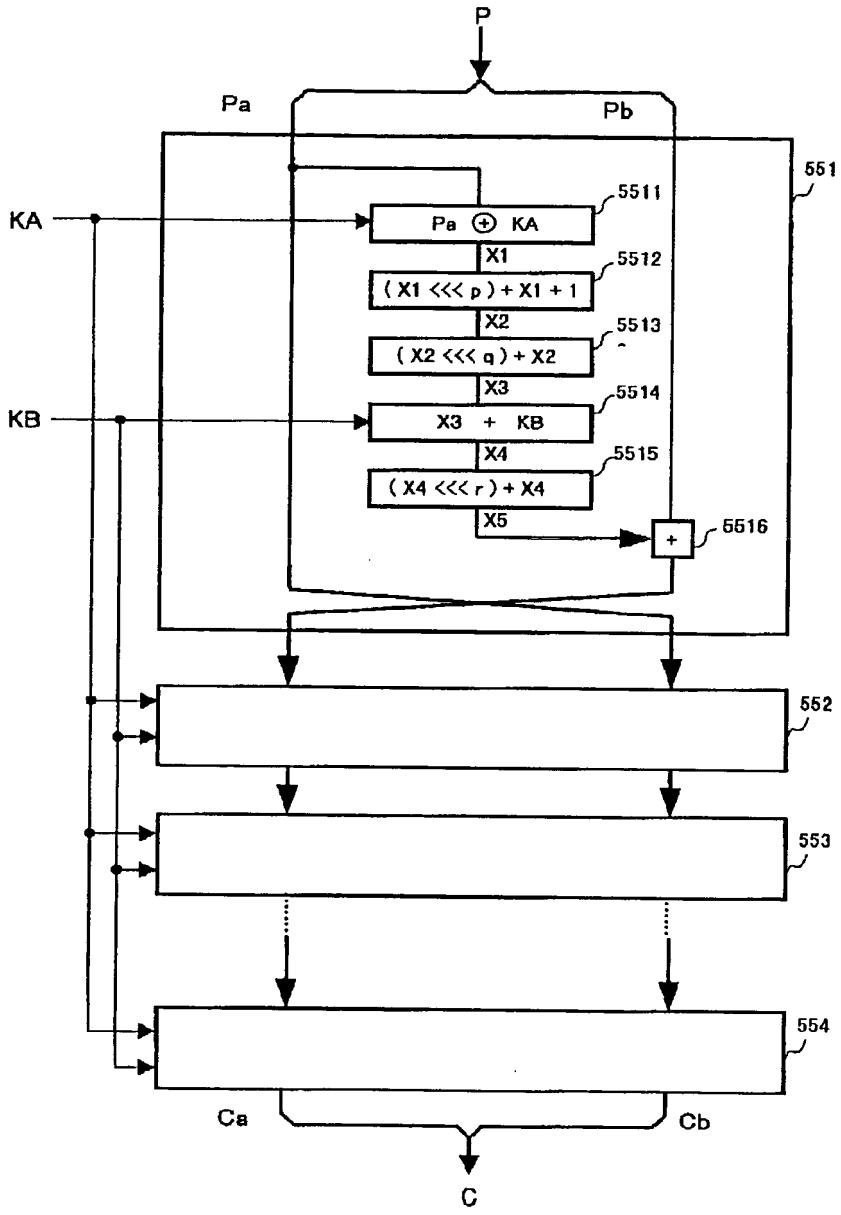
【図２６】

図２６



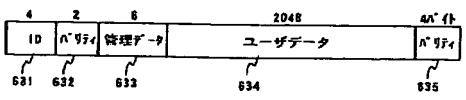
【図７】

図７



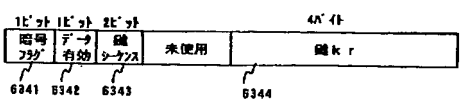
【図２９】

図２９



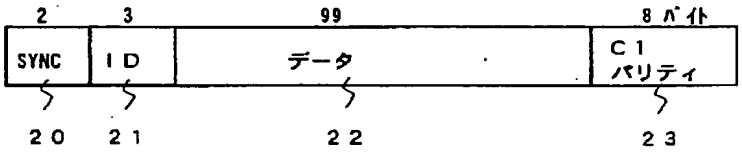
【図３３】

図３３



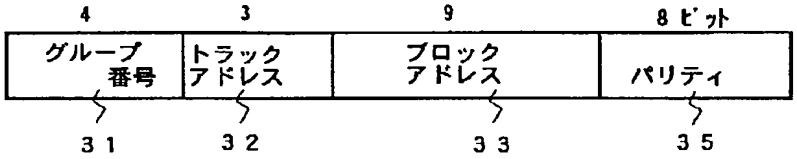
【図１０】

図１０



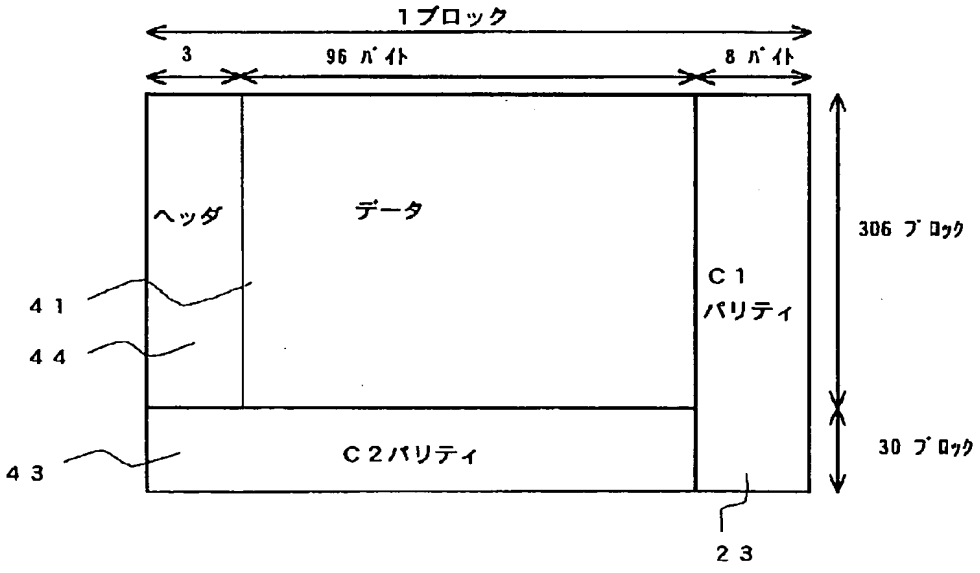
【図１１】

図１１



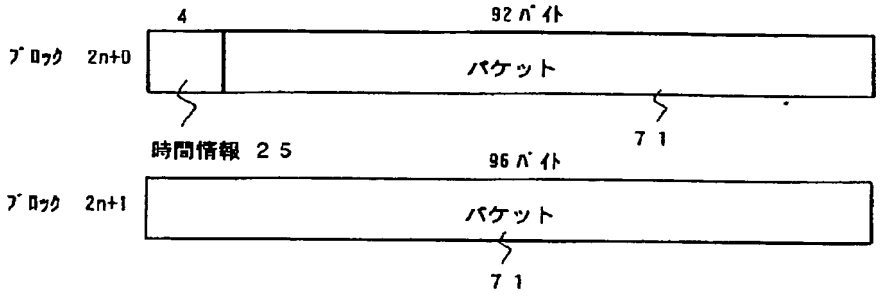
【図１２】

図１２



【図１３】

図１３



【図１６】

図１６

(1)

6a	“鍵情報”		
6a+1	“2”	“0”	“0”
6a+2	ブロック鍵 A0		
6a+3	ブロック鍵 A1		
6a+4	ブロック鍵 A2		
6a+5	ブロック鍵 A3		

6b	“鍵情報”		
6b+1	“1”	“0”	“0”
6b+2	ブロック鍵 A4		
6b+3	ブロック鍵 A5		
6b+4	ブロック鍵 A6		
6b+5	ブロック鍵 A7		

6c	“鍵情報”		
6c+1	“0”	“0”	“0”
6c+2	ブロック鍵 A8		
6c+3	ブロック鍵 A9		
6c+4	ブロック鍵 A10		
6c+5	ブロック鍵 A11		

(2)

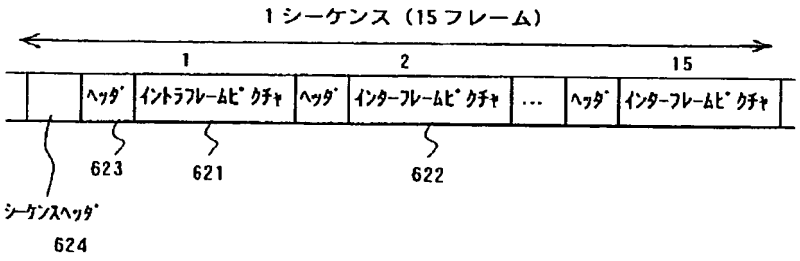
6d	“鍵情報”		
6d+1	“2”	“0”	“1”
6d+2	ブロック鍵 B0		
6d+3	ブロック鍵 B1		
6d+4	ブロック鍵 B2		
6d+5	ブロック鍵 B3		

6e	“鍵情報”		
6e+1	“1”	“0”	“1”
6e+2	ブロック鍵 B4		
6e+3	ブロック鍵 B5		
6e+4	ブロック鍵 B6		
6e+5	ブロック鍵 B7		

6f	“鍵情報”		
6f+1	“0”	“0”	“1”
6f+2	ブロック鍵 B8		
6f+3	ブロック鍵 B9		
6f+4	ブロック鍵 B10		
6f+5	ブロック鍵 B11		

【図２８】

図２８



【図１７】

図１７

(1)

6a	“鍵情報”		
6a+1	“2”	“0”	“0”
6a+2	ブロック鍵 A0		
6a+3	ブロック鍵 A1		
6a+4	ブロック鍵 A2		
6a+5	ブロック鍵 A3		

6b	“鍵情報”		
6b+1	“1”	“0”	“0”
6b+2	ブロック鍵 A4		
6b+3	ブロック鍵 A5		
6b+4	ブロック鍵 A6		
6b+5	ブロック鍵 A7		

6c	“鍵情報”		
6c+1	“0”	“0”	“0”
6c+2	ブロック鍵 A8		
6c+3	ブロック鍵 A9		
6c+4	ブロック鍵 A10		
6c+5	ブロック鍵 A11		

(2)

6d	“鍵情報”		
6d+1	“2”	“1”	“1”
6d+2	ブロック鍵 B0		
6d+3	ブロック鍵 B1		
6d+4	ブロック鍵 B2		
6d+5	ブロック鍵 B3		

6e	“鍵情報”		
6e+1	“1”	“1”	“1”
6e+2	ブロック鍵 B4		
6e+3	ブロック鍵 B5		
6e+4	ブロック鍵 B6		
6e+5	ブロック鍵 B7		

6f	“鍵情報”		
6f+1	“0”	“1”	“1”
6f+2	ブロック鍵 B8		
6f+3	ブロック鍵 B9		
6f+4	ブロック鍵 B10		
6f+5	ブロック鍵 B11		

(3)

6a	“鍵情報”		
6a+1	“2”	“0”	“1”
6a+2	ブロック鍵 B0		
6a+3	ブロック鍵 B1		
6a+4	ブロック鍵 B2		
6a+5	ブロック鍵 B3		

6b	“鍵情報”		
6b+1	“1”	“0”	“1”
6b+2	ブロック鍵 B4		
6b+3	ブロック鍵 B5		
6b+4	ブロック鍵 B6		
6b+5	ブロック鍵 B7		

6c	“鍵情報”		
6c+1	“0”	“0”	“1”
6c+2	ブロック鍵 B8		
6c+3	ブロック鍵 B9		
6c+4	ブロック鍵 B10		
6c+5	ブロック鍵 B11		

(4)

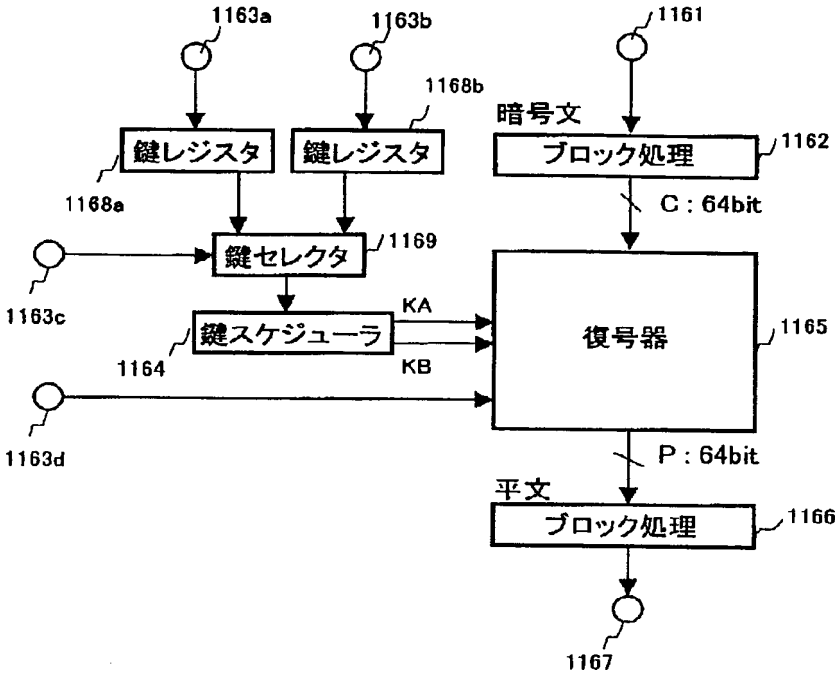
6d	“鍵情報”		
6d+1	“2”	“1”	“0”
6d+2	ブロック鍵 C0		
6d+3	ブロック鍵 C1		
6d+4	ブロック鍵 C2		
6d+5	ブロック鍵 C3		

6e	“鍵情報”		
6c+1	“1”	“1”	“0”
6e+2	ブロック鍵 C4		
6e+3	ブロック鍵 C5		
6e+4	ブロック鍵 C6		
6e+5	ブロック鍵 C7		

6f	“鍵情報”		
6f+1	“0”	“0”	“0”
6f+2	ブロック鍵 C8		
6f+3	ブロック鍵 C9		
6f+4	ブロック鍵 C10		
6f+5	ブロック鍵 C11		

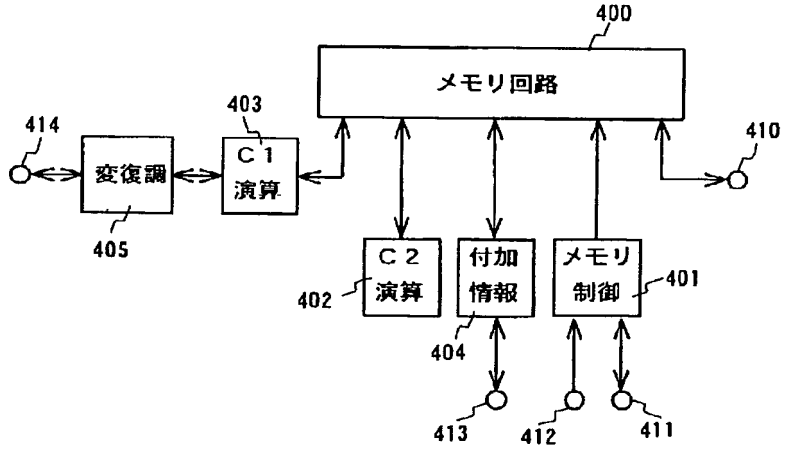
【図１９】

図１９



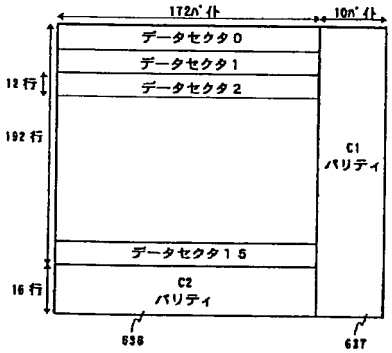
【図２０】

図２０



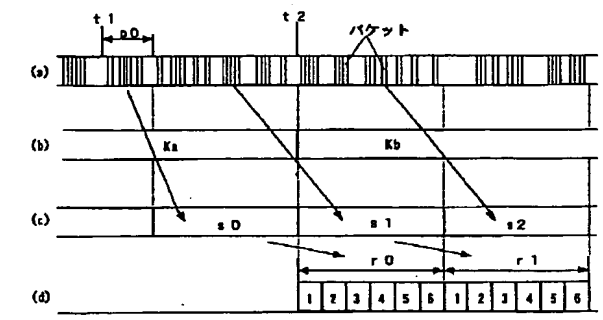
【図３０】

図３０



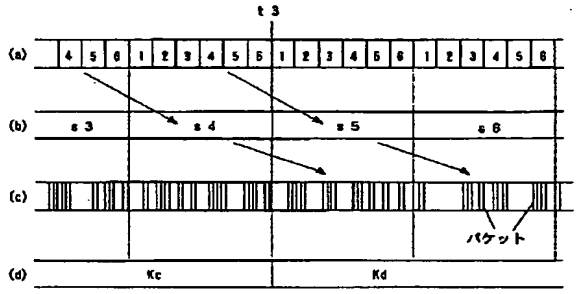
【図２１】

図２１



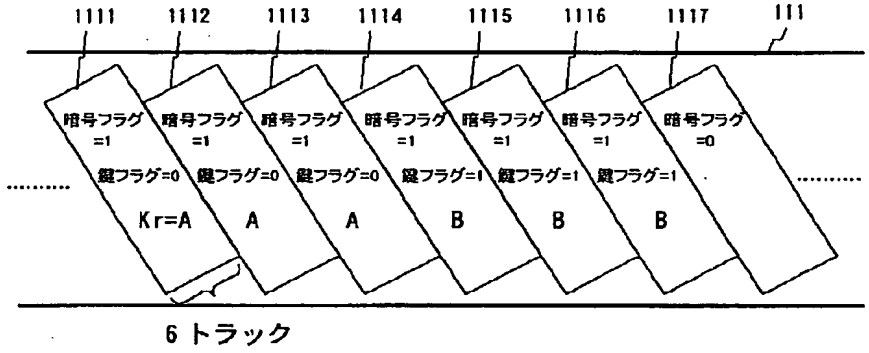
【図２３】

図２３



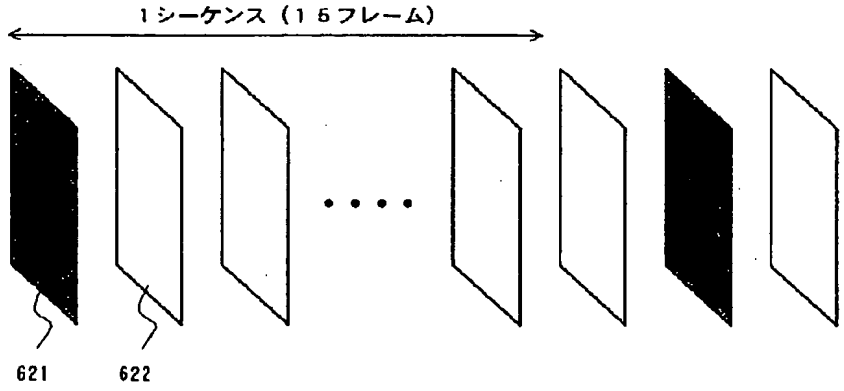
【図２２】

図２２



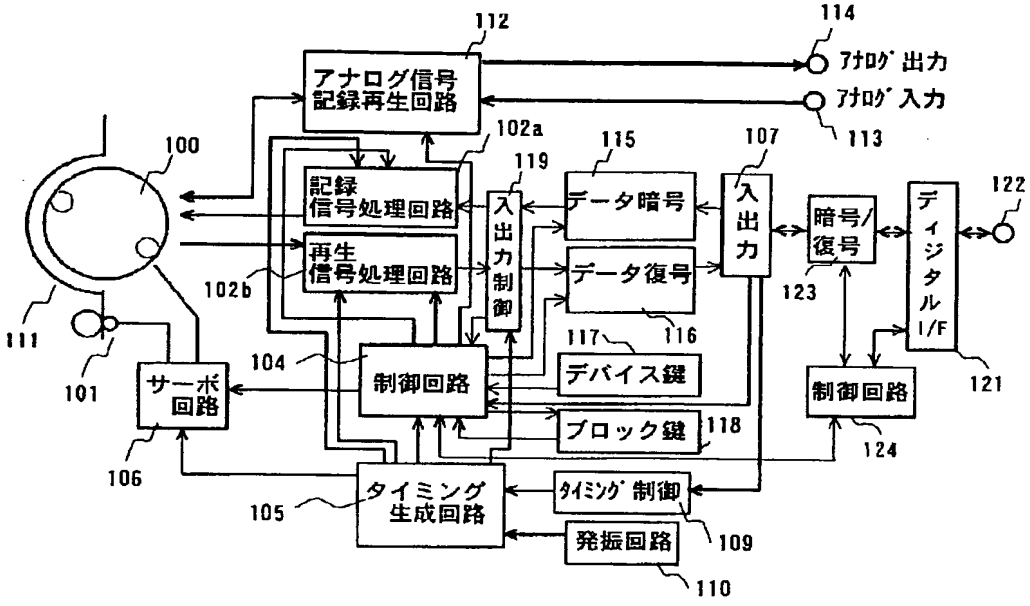
【図２７】

図２７



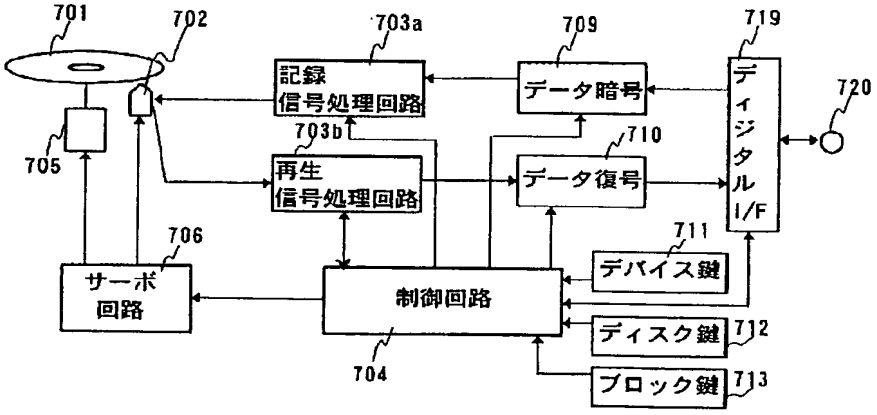
【図２４】

図２４



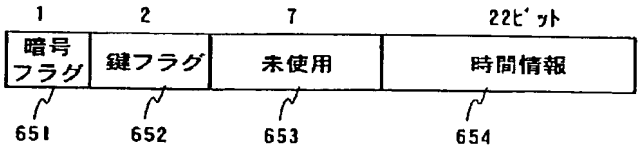
【図３１】

図３１



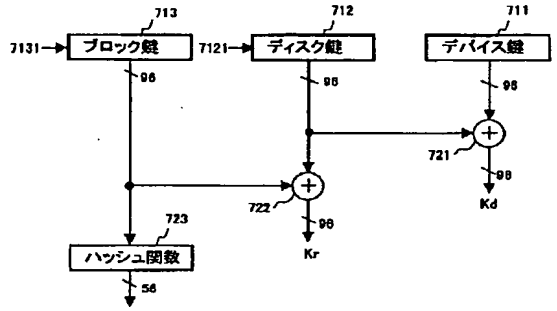
【図３７】

図３７



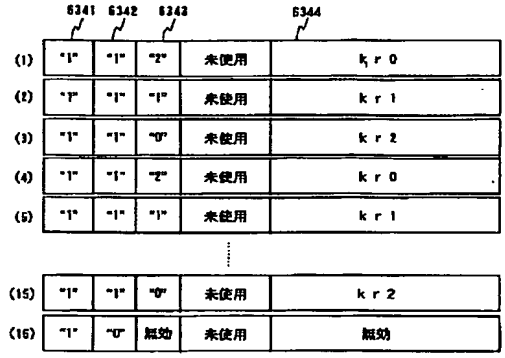
【図３２】

図３２



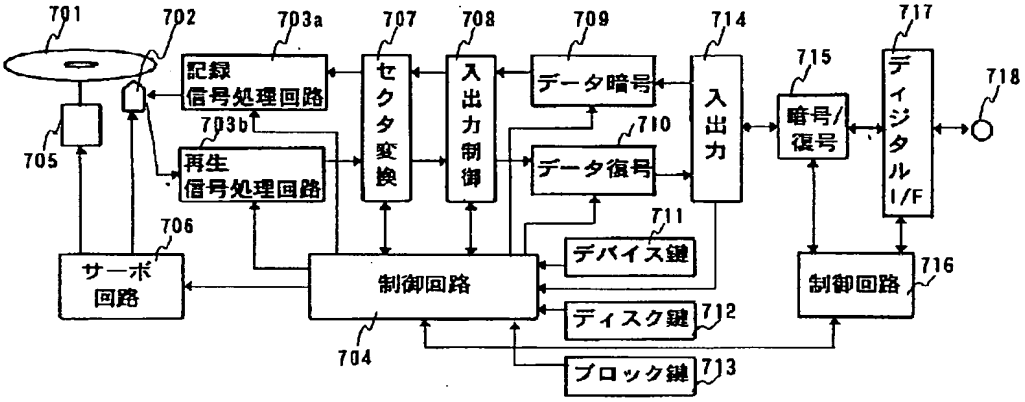
【図３４】

図３４



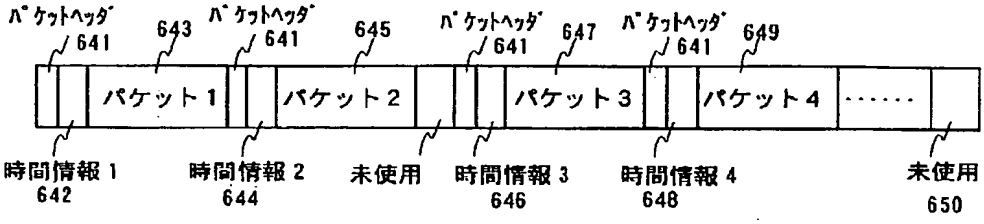
【図３５】

図３５



【図３６】

図３６



フロントページの続き

(72)発明者　千葉　浩
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　尾鷲　仁朗
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

Ｆターム(参考)　5C053 FA13 FA20 FA22 FA23 GB01 GB06 GB07 GB11 GB15 GB21 GB30 GB37 JA21 JA22 JA26 KA01 KA08 KA21 KA22 KA24 LA06 LA07
5D044 AB05 AB07 DE03 DE48 DE50 DE52 DE60 DE68 GK08 GK17